

# LANTRONIX®

**Spider™**

## SecureLinux Spider™ User Guide



Part Number 900-495  
Revision C May 2008

## Copyright & Trademark

© 2007, 2008 Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, Windows XP are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

### **LINUX GPL Compliance**

Certain portions of source code for the software supporting the SLS family are licensed under the GNU General Public License (GPL) as published by the Free Software Foundation and may be redistributed and modified under the terms of the GNU GPL. A machine readable copy of the corresponding portions of GPL licensed source code is available at the cost of distribution.

Such source code is distributed WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

A copy of the GNU General Public License is available on the Lantronix Web Site at <http://www.lantronix.com/> or by visiting <http://www.gnu.org/copyleft/gpl.html>. You can also obtain it by writing to the Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

## Contacts

### **Lantronix Corporate Headquarters**

15353 Barranca Parkway  
Irvine, CA 92618, USA  
Phone: 949-453-3990  
Fax: 949-453-3995

### **Technical Support**

Online: [www.lantronix.com/support](http://www.lantronix.com/support)  
Phone: (949) 422-7044  
(949) 453-7198

### **Technical Support Europe, Middle East, Africa**

Phone: +33 1 39 30 41 72  
Email: [mailto:eu\\_techsupp@lantronix.com](mailto:eu_techsupp@lantronix.com) or [mailto:eu\\_support@lantronix.com](mailto:eu_support@lantronix.com)

Firmware downloads, FAQs, and the most up-to-date documentation are available at <http://www.lantronix.com/support>

### **Sales Offices**

For a current list of our domestic and international sales offices, go to the Lantronix web site at [www.lantronix.com/about/contact](http://www.lantronix.com/about/contact).

## Disclaimer & Revisions

Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

**Note:** *This equipment has been tested and found to comply with the limits for Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this User Guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.*

*The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.*

Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Date	Rev.	Comments
3/07	A	Initial Document
11/07	B	Changed baud rate default to 9600; added Detector utility for assigning IP address; added ability to enable drive redirection, configure backup/restore, and reset factory defaults; introduced a CLI and commands.
4/08	C	Added Direct KVM; KVM-only mode; Spider network web page; ability to preserve network settings for factory defaults; country code support; iGoogle gadget; instructions for using the mounting kit.

# Contents

<b>1: Preface</b>	<b>6</b>
Purpose and Audience	6
Additional Documentation	6
<b>2: Introduction</b>	<b>7</b>
Features	7
Functionality	8
Technical Specifications	9
<b>3: Installation</b>	<b>11</b>
Package Contents	11
Configuration Planning	11
Batch vs. Individual Setup	12
Installation and Network Settings	13
Target Computer Setup	16
Client Setup	18
Network Environment	19
Power	19
<b>4: Web Browser Access</b>	<b>20</b>
<b>5: Remote System Control</b>	<b>22</b>
KVM Console	22
Telnet/SSH	29
<b>6: Interfaces</b>	<b>32</b>
Network Settings	32
Serial Port Settings	34
KVM Console Settings	35
Keyboard/Mouse	39
Video	41
Virtual Media	42
<b>7: User Accounts</b>	<b>49</b>
Local vs. Remote Authentication	49
Local User Management	49
User Permissions	51
Remote Authentication	52

<b>8: Services</b>	<b>55</b>
Date/Time _____	55
Security _____	56
Certificate _____	58
Event Log _____	60
SNMP _____	61
Spider Network _____	62
<b>9: Maintenance</b>	<b>64</b>
Device Status _____	64
Configuration _____	65
Update Firmware _____	66
View Event Log _____	67
Unit Reset _____	67
iGoogle Gadgets _____	68
<b>10: Command Line Interface (CLI)</b>	<b>70</b>
Introduction to Commands _____	70
Configuration Commands _____	72
Connect Commands _____	72
SSH Key Commands _____	72
History Commands _____	74
Network Commands _____	74
Version Command _____	75
<b>A: Troubleshooting</b>	<b>76</b>
<b>B: Virtual Media Example</b>	<b>78</b>
Goal _____	78
Step 1 – Prepare the VM Server _____	79
Step 2 – Enable Virtual Media _____	80
Step 3 – Use the Virtual Media _____	81
<b>C: Supported Video Formats</b>	<b>83</b>
<b>D: Mounting Bracket Kit for the Spider (083-015-R)</b>	<b>84</b>
<b>E: Technical Support and Warranty</b>	<b>85</b>
Technical Support _____	85
Warranty _____	85
<b>F: Compliance</b>	<b>86</b>

# 1: Preface

## Purpose and Audience

This guide describes how to install, configure, use, and update the SecureLinx Spider device. It is for users remotely and securely monitoring and control of one target computer system by one or more remote users.

## Additional Documentation

The following guide is available on the product CD or the Lantronix Web site:  
[www.lantronix.com](http://www.lantronix.com).

Document	Description
Spider View User Guide	Details instructions on using the Spider View utility.
SecureLinx Spider Quick Start Guide	Provides an overview of using the Spider.

## 2: Introduction

This chapter introduces the Lantronix SecureLinx Spider (SLS) line of KVM-over-IP devices. It provides an overview of the products, lists their key features, and describes the applications for which they are suited.

The SecureLinx Spider is a distributed KVM-over-IP device designed to remotely and securely provide monitoring and control of one (target) computer system by one or more remote users. The remote user (client) accesses the Spider over a local or wide area network connection using a standard web browser. The Spider provides secure, remote IP-based access to Keyboard, Video, and Mouse (KVM) on the attached server, and makes it available to anyone who can access the Spider's IP address. Spider is an evolution of the traditional remote KVM switch into a compact package. It is light enough to be cable-supported from the back of a server and takes up no rack space.

There are four models: one with both PS/2 and USB keyboard/mouse interfaces (software selectable), one for USB-only systems, and two variations of cable length (21" and 58") for each. The Spider is unique in that it is low-enough in power consumption to be powered from the attached server. The color-coded plugs on the ends of the cables for the keyboard, mouse, USB port and video are designed to plug directly into the target system's corresponding connectors. An optional external AC/DC power supply is available.

The Spider differs from other KVM-over-IP switches in several ways. Unlike rack mount KVM-over-IP switches, the allocation of one Spider per computer allows *add-as-you grow* scalability and guarantees non-blocked BIOS-level access to mission-critical servers regardless of the number of remote users or servers that need access. Also, Spider is unique in that it uses Lantronix SwitchPort+ technology to incorporate two hardware-switched Ethernet ports, one for the primary network connection and the second for daisy-chaining Spiders, or aggregating other Ethernet connections (for example, a dedicated management LAN port on the controlled system). This provides a cost-effective solution in environments where numerous cable drops and distance limitations can be a challenge when adding servers.

## Features

- ◆ Secure, full BIOS-level control of remote servers over an IP network
- ◆ Space saving "zero footprint" package attaches directly to the server – saves rack space
- ◆ Flexible 1 port design allows you to scale as you grow
- ◆ Server-powered design - no external power supply required
- ◆ Guaranteed non-blocked access to remote servers – ensures lowest "cost-per-remote user"
- ◆ Browser based - no client software or special licensing required

- ◆ No video degradation with long Cat-5/6 cable runs (up to 300 feet) - eliminates cable distance limitations of typical rack-mounted analog/CAT5 KVM switches
- ◆ Lantronix SwitchPort+ technology allows Spiders to be cascaded or share a host's Ethernet connection
- ◆ Virtual Media support allows local drives (floppy, CD, hard drive, USB stick) to be shared with the remote server or to remotely install an O/S from an .ISO image
- ◆ *Direct KVM* minimizes the number of clicks to the remote server's console
- ◆ Built-in RS-232 serial port can be configured for serial console pass-through or remote dial-in access
- ◆ Ideal for Distributed IT systems environments such as small branch offices, campuses, test labs, and server hosting environments

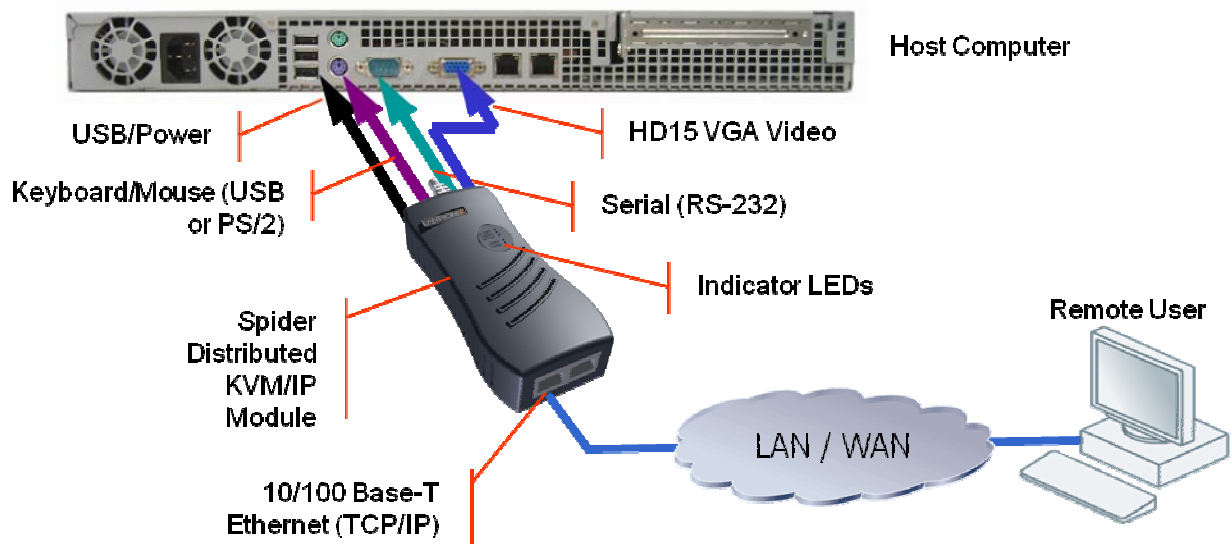
## Functionality

The Spider contains an embedded web server, dedicated hardware, and control firmware that:

- ◆ Captures the video output from the attached computer.
- ◆ Compresses the video and serves it up over the network to a Java KVM console window launched by the browser or to a command line on the user's system, which draws a replica of the server's video output on the user's monitor.

The Java KVM console then

- Accepts keystrokes and mouse movements on the user's system.
- Recognizes those intended for the target computer.
- Transmits those to the Spider.
- Emulates a physically attached keyboard and mouse to spoof the computer into thinking the user is sitting next to it

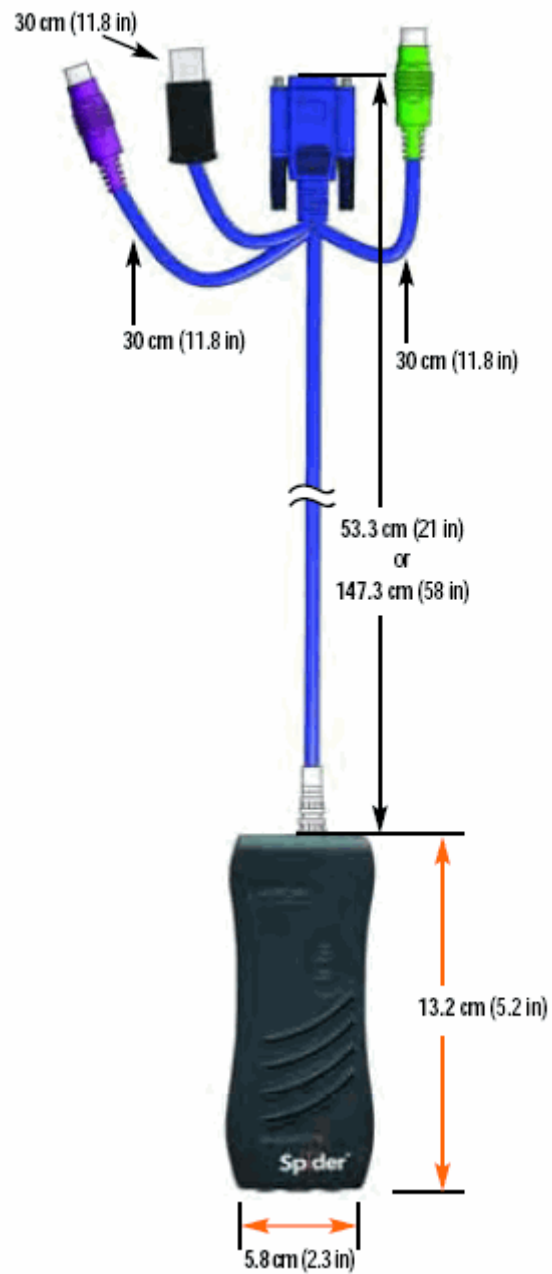




## Technical Specifications

<b>Security</b>	<ul style="list-style-type: none"> <li>– Secure encryption of keyboard, mouse, and video data</li> <li>– IP Source Address Filtering</li> <li>– Remote Authentication: LDAP, RADIUS, Active Directory</li> <li>– User/Group management with permissions control</li> <li>– Configurable port numbers (HTTP, HTTPS, Telnet, SSH)</li> <li>– Selective disable of Telnet/SSH</li> </ul>
<b>Target Server Requirements</b>	<ul style="list-style-type: none"> <li>– Supports Multiple Operating Systems: Windows 98/2000/2003/XP/Vista, Unix, Linux, or MAC OSX 10</li> <li>– Power/keyboard/mouse: 2 USB ports; or 1 USB and 1 PS/2 keyboard and 1 PS/2 mouse connector</li> <li>– Video Interface: HD15 VGA video output (up to 1280x1024@60Hz)</li> </ul>
<b>Client System Requirements</b>	<ul style="list-style-type: none"> <li>– Internet Explorer 6.0+, Netscape 5.0+, Mozilla 1.0+, FireFox 1.0+, Safari 2.0+</li> <li>– PIII Processor equivalent or better (recommended)</li> <li>– Sun (JRE) Java Runtime Environment 1.4 or later</li> <li>– Telnet/SSH client for command line (CLI) access</li> </ul>
<b>Optional Items</b>	<ul style="list-style-type: none"> <li>– Optional DC power supply with international adapters (100-240VAC, 50-60 Hz; 5 VDC @ 1A; USB “Mini-B” Type jack)</li> <li>– Replacement mounting bracket kit (see Appendix D)</li> </ul>
<b>Interfaces</b>	<ul style="list-style-type: none"> <li>– Network: One 10/100Base-T Ethernet Port with activity indicators (RJ45)</li> <li>– Cascade: One 10/100Base-T Ethernet Port with activity indicators (RJ45)</li> <li>– Serial: RS-232, up to 115,200 bps</li> <li>– Keyboard/Mouse: PS/2 or USB</li> <li>– Video: HD15 VGA</li> </ul>
<b>Environmental</b>	<ul style="list-style-type: none"> <li>– Operating: 0° to 45° C (32° to 115° F)</li> <li>– Storage: -20° to 70° C (-4° to 158° F)</li> <li>– Humidity: 0 to 95% RH (non-condensing)</li> <li>– Heat Dissipation: 4 Watts (14 BTU/hr)</li> </ul>
<b>Power Requirements</b>	<ul style="list-style-type: none"> <li>– Input: 5 VDC @ .8A max. (server powered)</li> <li>– Optional Auxiliary DC power supply available for redundancy</li> </ul>
<b>Dimensions (H x W x D)</b>	<ul style="list-style-type: none"> <li>– 13.2 x 5.8 x 3.1 cm (5.2 x 2.3 x 1.2 in)</li> <li>– Refer to Figure 2-1 for cable dimensions.</li> </ul>
<b>Weight</b>	<ul style="list-style-type: none"> <li>– 185g (6.6 oz)</li> </ul>
<b>Shipping Weight</b>	<ul style="list-style-type: none"> <li>– .5 kg (1.0 lbs)</li> </ul>

Figure 2-1 Spider Cable Dimensions



## 3: Installation

This chapter describes how to install the SecureLinx Spider.

### Package Contents

In addition to the Spider distributed KVM/IP module, the box contains the following items:

- ◆ Null modem DB9F to RJ45 serial cable
- ◆ Mounting kit (For details, see *D: Mounting Bracket Kit for the Spider (083-015-R)*.)
- ◆ Quick Start Guide
- ◆ CD-ROM containing documentation and utilities

An optional external AC/DC power supply is available.

### Configuration Planning

Consider the following factors when determining how to use the Spider in an environment:

#### Keyboard/Mouse Interface

The USB interface is typically preferred as it provides better remote cursor tracking. Some older systems do not have BIOS supporting USB human interface devices or there may not be two available USB ports. In these cases, the PS/2-interface model may be required; note that for this model the USB or PS/2 interface keyboard/mouse may be selected via software.

#### Spider Serial Port

The RS-232 port on the Spider is used for initial configuration of setup parameters, but it can subsequently be used to connect to a target's COM port. The Spider allows remote users to Telnet or SSH to that port, eliminating the need for a separate box to perform serial command line management. Alternatively, the serial port can be used for PPP connection to the Spider's user interface so that remote users can access the Spider via a modem or other serial interface. This could be either the primary network connection or a backup in case the primary LAN connection is unavailable.

#### Redundant Power

The Spider draws all of its power from the attached server, eliminating the need for external power supplies. Note that if the server loses power, the Spider loses power as well. With an optional auxiliary DC supply fed from an independent AC power source, the Spider will always have power regardless of the state of the server.

## Second Ethernet Port

The Spider incorporates a hardware Ethernet switch connecting the external two ports and the internal CPU for many possible configurations. The first port is required for connection to the network.

Potential uses for the second Ethernet port:

- ◆ Tying all the Spiders in a rack together so that only one external network connection is required. While this configuration physically is a chain, logically each Spider is addressed directly from the outside network. Because the data from the Spider at the end of the chain does need to traverse the entire series of switches, latency increases and hence responsiveness degrades with the number of devices. A maximum of 16 Spiders in a chain is recommended, though this is a function of the type of application and acceptable level of response. If the switch to which the Spider chain is networked supports Spanning Tree, the first and last devices in the chain may both be connected to the same switch to provide resilience against a single point failure.
- ◆ Connecting to the attached server's LAN management port; an external management network can then interface to both the Spider and the server via one cable.
- ◆ Connecting to the attached computer's main LAN port. If physical isolation of management data and user data is not a concern, a single LAN cable can provide connectivity to both Spider and computer, conserving a switch or router port.
- ◆ Aggregating any other Ethernet connection as a general-purpose switch port.

## Batch vs. Individual Setup

It may be necessary to deploy a batch of Spider devices at once. In that case, stage them on a bench for pre-configuration before attaching them to their respective computers. Some tips for configuring a batch of Spiders:

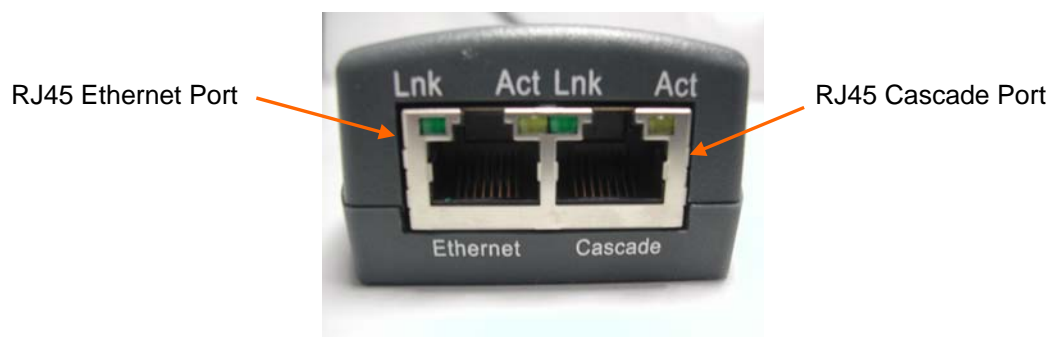
- ◆ The keyboard/video/mouse connections are not required for setup. All you need are a source of power and a serial connection to set up the network parameters, and an Ethernet connection to access the administration user interface.
- ◆ The quickest and easiest source of power is the auxiliary DC input. DC supplies are available from Lantronix under order number 520-085-R. If using a third party charger with mini-USB connector, make sure it is 5V@1A regulated ("Efficiency level III" or "IV" is an indicator that it is a switching supply and hence well regulated) with an adequate cable.
- ◆ Tag each Spider with its IP address or write it on the serial number label on the bottom.

## Installation and Network Settings

Figure 3-1 Serial and Auxiliary Power Port



Figure 3-2 Ethernet and Cascade Ports



### Indicator LEDs

<b>Pwr1</b>	Blue	Power Good indicates adequate power from source 1 (USB1)
<b>Pwr2</b>	Blue	Power Good indicates adequate power from source 2 (USB2 or PS/2)
<b>SysOK</b>	Green	Blinks upon bootup. Steady when up and healthy
<b>Video</b>	Green	Video is coming from target server (Vsync present)
<b>Unit ID</b>	Orange	Optionally lit to assist in finding unit

1. Plug the RJ45 end of the included serial cable into the Spider's serial port. Plug the DB9F end into the serial (COM) port of a PC/laptop running a terminal emulation (e.g., HyperTerminal). The default serial port settings are 9600 bits per second, 8 data bits, no parity, 1 stop bit, no flow control.
2. The Spider is typically powered by the attached server. Plug the Spider video, USB, and PS/2 keyboard/mouse (if applicable) cables into the target computer (this is required for the device to boot up). The two blue power LEDs will illuminate and the green system OK LED flashes to indicate that it is booting up. Bootup is complete within approximately one minute. The system OK LED stops flashing and remains illuminated.

3. Upon bootup, the terminal window displays the login prompt. To change the default IP auto configuration from DHCP to a static IP address, type **config** and press **Enter**.
4. At the IP autoconfiguration prompt, type **none** and press **Enter**.

```
Welcome!
Choose a login for the following features:
-Initial IP configuration: "config".
-Reset device: "reset".
<none> login: config
IP autoconfiguration <none/dhcp/bootp> [dhcp]: none
```

5. Follow the prompts to enter the unit's IP address, subnet mask, default gateway, and LAN interface information.

```
IP [192.168.1.22]:
NetMask [255.255.255.0]:
Gateway <0.0.0.0 for none> [0.0.0.0]:
LAN interface speed <auto/10/100> [auto]:
LAN interface duplex mode <auto/half/full> [auto]:
Are the entered values correct? Enter y for Yes, n for No or c to Cancel y
Configuring device ...
Done.
```

6. Type **y**, following by **Enter**, to accept the changes. The system takes several seconds to update the internal protocol stack and display the updated information.
7. Plug an Ethernet cable connected to your network into the Ethernet port. The Link LED illuminates.

## Assigning a Static Address with Detector

The Detector software is on the product CD. Use Detector to replace an automatically assigned IP address with a static IP address.

**Note:** If you try to run **detector2.exe** on a network shared drive, you may get a security exception. We recommend that you run the program on the CD or copy the **detector2** directory to your local hard drive and run it from there. If you must run **detector2.exe** from a network shared drive, you need to change your security settings using the ".NET Framework Configuration" or "caspol" tool.

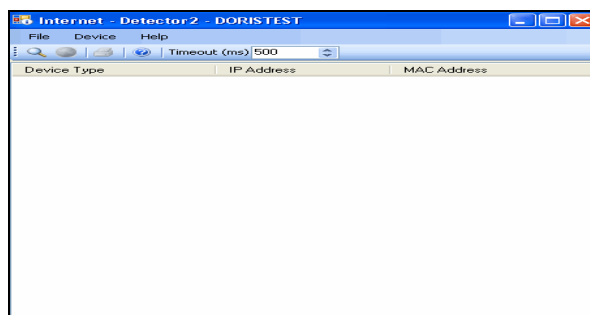
### To install .NET required by the Detector:


1. Double-click **detector2.exe** on the product CD.
2. If a "The application failed to initialize properly (0xc0000135), click **OK** to terminate the application" message displays, you need to install .NET Framework.
3. Obtain the .NET Framework redistributable package from the Spider CD. It is also available as a stand-alone executable file, **Dotnetfx.exe**. You can download this from Microsoft at:

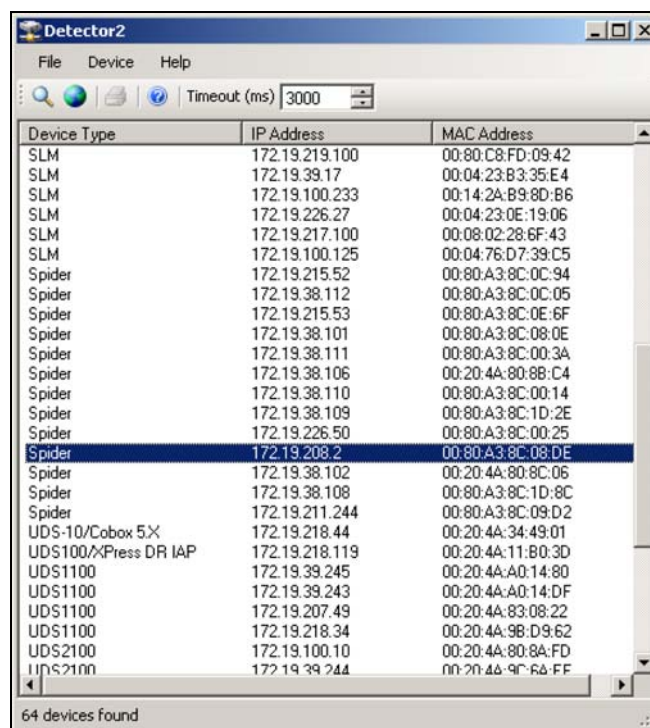
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>

**To use Detector to set the IP address:**

1. Open the Detector software. The Lantronix Detector window opens.

**Lantronix Detector Window**

2. From the **Timeout** drop-down menu (in the toolbar), select the number of milliseconds before the search stops. The default is **3000**.
3. Click the **Search** icon . A list of Lantronix Ethernet devices on the network displays.

**Detector Device List Window**



4. If the Spider has an automatically assigned IP address and you want to change it, select the Spider and click the **Network Settings** icon . The Enter Network Settings window displays.

Figure 3-3. Network Settings Window

The **Device Type** and **MAC Address** (Ethernet Address) fields identify the unit.

5. Enter the following information:

<b>IP Address</b>	An IP address that will be unique and valid on your network and in the same subnet as your PC. There is no default. <b>Note:</b> Enter all IP addresses in dot quad notation.
<b>Subnet Mask</b>	The subnet mask specifies the network segment on which the Spider resides. To accept the default, leave blank.
<b>Default Gateway</b>	IP address of the router for this network. To accept the default, leave blank.

6. Click **OK**. A message confirms that your network configuration was sent.
7. Click **OK**.
8. To confirm the change, click the **Search icon**  and verify that the unit has new network settings.

**Note:** On the **Interfaces**→**Network** page of the web interface, make sure **Disable Setup Protocol** is **not** selected in the Network Miscellaneous Settings section.

You can now access the unit using the new IP address.

## Target Computer Setup

### Video

The Spider recognizes a wide variety of VESA, Sun, and Apple video resolutions up to a maximum of 1280x1024@60 Hz; the complete list of supported video formats is in [C: Supported Video Formats](#).



To minimize power consumed in the server and attached Spider, set the monitored server's video resolution to the minimum necessary for your remote monitoring application.

We recommend 1024x76 or 800x600 if connecting the Spider over a wide area network rather than a LAN. 1280x1024 may be used for applications demanding higher resolution; however it consumes more network bandwidth. The other supported formats are recognized by the Spider, but may offer difficulty if the timing does not comply with the applicable standard. The Spider supports the extended display identification data (EDID) standard for informing the attached computer of its supported video formats.

- ◆ On a Windows target system, select **Control Panel→Display→Settings**. Modify the screen resolution value as necessary.
- ◆ Select **Control Panel→Display→Settings→Advanced→Monitor**. Modify the screen refresh rate (consult the appropriate documentation when using an atypical video card or another operating system on the target computer). Since the server's video output is driving the Spider and not a monitor, a refresh rate higher than 60 Hz has no effect.
- ◆ For Linux systems, edit the Xfree86 file XF86Config to disable formats that are not supported or not VESA standard timing; a reboot is required.

If you are using a special video card or another operating system on the target, consult the appropriate documentation.

Solaris servers may need to be set to output H+V sync, not composite sync. The power-down-monitor settings in the operating system's power management have no effect on the Spider's internal operation and network interface, but if the attached server is in a monitor power-down mode the client application displays "No Video" and the Video LED will be out. The "Video" LED on the Spider actually monitors the vertical sync signal, not the video data itself.

Background wallpaper and desktop appearances do not have any particular limitations, although Microsoft Active Desktop and Linux graphical interfaces' virtual desktop are not supported. If bandwidth is a concern, plain backgrounds are preferred.

## Mouse

Mouse to cursor synchronization has long been a troublesome issue with digital KVM interfaces. PS/2 mice transmit incremental information about movement over a period of time, not an absolute measurement; the driver in the operating system then translates to distance based on the local screen resolution and applies linear or nonlinear acceleration mappings. When a remote client system is communicating with the target system, settings and screen resolutions on both sides of the connection must be taken into account in order to get natural mouse-to-cursor tracking. Use the USB keyboard/mouse when supported by the target computer. Unlike the PS/2 interface, a USB mouse uses absolute coordinates rather than relative coordinates and hence does not present the difficulties in translation between local and remote systems. On the PS/2 model Spider, when the keyboard/mouse interface is set to Auto it will first attempt to use the USB interface and only if it does not detect support in the attached OS will it fall back to PS/2.

There are no restrictions on the mouse settings of the client systems. And as a rule, no special care must be taken on setting mouse parameters of target systems when using the USB mouse interface. For the PS/2 interface, performance (tracking) and synchronization can be optimized by removing any special acceleration or nonlinear ballistics. For several common operating systems:

- ◆ On a Windows target system, select **Control Panel→Mouse→Pointer Options**. Set the pointer speed to medium and disable **Enhanced pointer precision**.
- ◆ Linux graphical interfaces. Set Mouse Acceleration to exactly 1 and threshold to exactly 1. Also, select **Other Operating Systems** on the Spider mouse settings page.
- ◆ Sun Solaris. Adjust mouse settings via the CDE control panel to “1:1, no acceleration” or via “xset m 1”.
- ◆ Mac OS X. Set Spider to **Single Mouse Mode**.

## Serial

If you plan on using the Spider to Telnet or SSH to the target system's serial port, set that port to match the Spider's equivalent settings. The Spider's default serial settings are 9600 bps, 8 data bits, 1 stop bit, no parity, and no handshake. The pinout of the included cable matches a standard DB9 COM port.

## Cabling

Connections for video, USB, and keyboard/mouse are integrated into the Spider. Do not use extension cables; plug the Spider directly into the appropriate ports on the host system. If using the serial port, cable it to the appropriate COM port on the server. The second Ethernet port (cascade) may be used to connect to the target computer's management LAN port or main LAN port, or to chain Spiders. When connecting the Ethernet ports, either straight through or crossover cables may be used, as the Spider has both auto-polarity and auto-crossover correction. Although both the port marked Ethernet and the port marked Cascade are Ethernet interfaces, you must use the port marked Ethernet if using only one Ethernet interface.

- ◆ When chaining Spiders, bring the outside network cable in to the left Ethernet port of the first Spider.
- ◆ Connect the right Cascade port to the left port of the next Spider in the chain.
- ◆ Repeat as necessary. The last Spider in the chain will have its right port unoccupied, unless cabling in a loop for redundant connection.

The downside to chaining Spiders is that a break in the cabling or device failure results in a loss of network connectivity for all Spiders downstream of the fault. This can be averted if the switch or router to which the Spider chain attaches supports Spanning Tree, and has it activated. In that case, the last Spider can have its Cascade port tied back to the same switch so that there is a redundant outside connection. The Spanning Tree protocol implemented in the switch will disable one of the two network connections while the loop remains complete; data will flow in only one direction around the loop. If the loop is broken, it activates both connections, so that data can flow in both directions. All Spiders will be accessible except the one immediately downstream from the break or down unit. Do not try this without Spanning Tree in place.

## Client Setup

Two mechanisms are provided for monitoring Spider-connected targets at client systems. Spider View is a standalone Windows application that can locate, manage, and access multiple Spiders from an integrated view. Spider View requires a client to be running Windows XP or later and have ActiveX controls enabled. Please refer to the separate Spider View User Guide for instructions on installation and operation of Spider View.

For platform-independent management, each Spider contains an embedded web server that delivers web pages, a Java KVM remote console program, and a terminal program. The client system must have a web browser (Spider supports browsers such as Internet Explorer 6.0+, Netscape 5.0+, FireFox 1.0+, and Safari 2.0+) in order to access and administer the Spider. To run the actual Remote Console window and manage the target system, a Java plug-in is also required. To run the actual Remote Console window and manage the target system, a Java plug-in (Sun JRE 1.4 or later) is also required.

## Network Environment

The connection between client and Spider must be open to IP traffic and have TCP ports 80 (HTTP) and 443 (HTTPS) open. Firewalls and NAT devices may need to be configured to support this; consult your system administrator. The TCP ports used by the Spider may be changed at **Interfaces→Network**.

When idle, the Spider generates minimal network traffic but when images are rapidly changing on the host system and image quality is set to the maximum there can be bursts of traffic exceeding 10 mbps; fast Ethernet connections are recommended. In a local area network, the responsiveness of the Remote Console window will be affected by traffic; a switched network environment is advised.

## Power

The Spider is low enough in power consumption (under 4 watts) to draw its power from the attached computer. However, it requires all cables to be plugged in to receive sufficient power. Plug in both USB cables or a USB and a PS/2 cable. The Pwr1 LED indicates that power is available on the first USB port. The Pwr2 LED indicates that power is available the second USB port, or the PS/2 ports. The Spider will not start up until both Pwr1 and Pwr2 LEDs are on. It then begins to blink the SysOK LED, which will continue to blink while the boot process continues. The Spider is Linux-based, and takes about a minute to boot. When the SysOK LED is on steady, the Spider is up and ready to communicate.

The Spider can also derive power from an external DC supply. DC supplies are available from Lantronix under order number 520-085-R. The DC supply is most useful as a backup, as the Spider will otherwise lose power if the attached computer does.

In addition to power-on reset, the Spider can also be rebooted from the user interface, from the serial port, or by clicking the reset switch through the pinhole on the back of the body.

## 4: Web Browser Access

The SecureLinx Spider controls a target computer by redirecting its human interface peripherals of keyboard, mouse, and video screen to one or more other (client) computers. The Spider achieves this by serving up web pages and launching a Java KVM console across the network connection to the client using standard protocols (such as IP, TCP, and HTTP/HTTPS). The Java KVM console window running on the client system appears as a preview of the target computer's screen.

**Note:** The Spider supports browsers such as Internet Explorer 6.0+, Netscape 5.0+, FireFox 1.0+, and Safari 2.0+.

When using the Spider View application on Windows, refer to the [Spider View User Guide](#). This section refers to the Spider connection via a web browser.

1. Access the Spider over the network using a web browser by entering: **https://** (for a secure SSL connection) or **http://** (for an insecure connection) and its IP address in the address bar. The browser must accept cookies for login.
2. Enter your user name (default is **sysadmin**) and password (default is **PASS**) at the prompt. The Spider home page displays.



After passing authentication, the Spider opens the home page, from which the Remote Console or Telnet Console may be launched. The home page contains a snapshot of the target system's video in the Remote Console Preview window, various pieces of information (session and host name), a series of tabs along the top left, and buttons, including a **Logout** button, along the top right.

At this point, you are logged in with all permissions to make changes to configuration and user database. You may then set the unit up for either local or remote authentication for other users, and define their permission level. As sysadmin, you may also make changes to the hardware settings, establish configuration parameters, and perform maintenance operations.

## 5: Remote System Control

The Spider's primary function is running the Remote Console (Remote Console). The Remote Console window has settings that apply each time a user launches it. Other settings may be applied within the window itself. By scaling the window down in size, it is possible to have multiple Remote Console windows open, allowing interaction with multiple target systems.

### KVM Console

#### To launch the Remote Console window:

1. Click the **KVM Console** button to launch the Lantronix Spider Remote Console. The Remote Console window may open in the foreground or in the background. If it launches in the background, click on the icon to bring the window to the front.

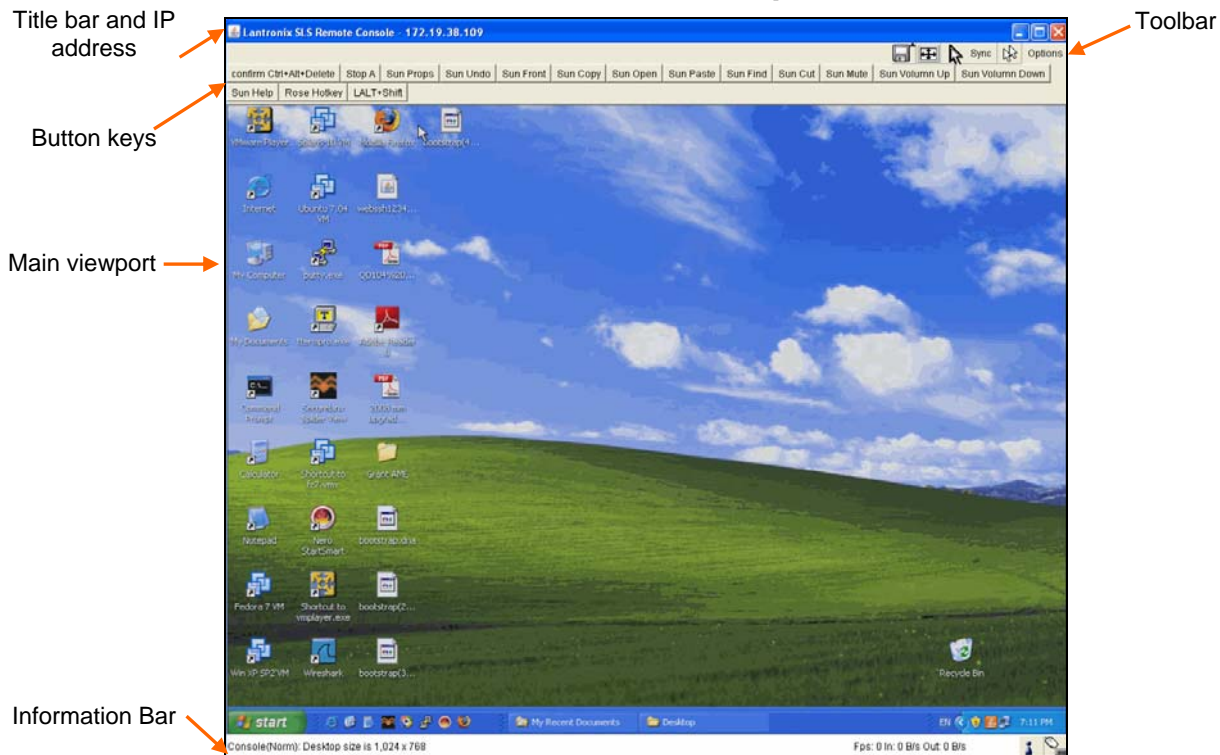
Alternatively, launch the Remote Console by clicking the link below the preview image on the **KVM Console Preview** window.

**Note:** You can enable the Spider to bypass the web page and take you directly to the remote system. This capability is called *Direct KVM*.

The Remote Console window shows a real-time replica of the video output from the target system (mimicking a monitor plugged directly into the remote computer). When the local computer's focus is within the Remote Console window, mouse movements and keystrokes are transmitted to the remote computer. The title bar of the window shows the IP address of the Spider providing this view (useful when multiple windows are open on the client system).

The Remote Console window is like any other window on the client system. It may be minimized, maximized, or scaled in either direction.

## Console Window Components



### Main Viewport and Scroll Bars

When first launched, the full virtual screen of the target computer is mapped pixel-for-pixel to the console window's main viewport. As a result, if the target is running at a resolution less than that of the client, the entire screen is visible in the Remote Console window. If the resolution is such that the screen does not fit, scroll bars are available in the Remote Console window to move the viewport around within the target's screen. The virtual screen size of the target may also be scaled down to match the Remote Console window.

### Button Keys

Along the top there are Button Keys that have been defined to send special key codes directly to the target computer.

### Toolbar

The top toolbar has a number of buttons for one-click access to functions, and a drop-down menu where other options may be reached. The icons vary depending on which keyboard interface is active.

### Access Virtual Media

The leftmost diskette icon is used to activate the Virtual Media toolbar.

### ***Auto Adjust Video***

This button activates the Auto Adjust Video function. When first opening the Remote Console window, it is recommended to click this button to ensure the Spider has locked on to the video format on the attached computer. Also, click this button if there is an offset from the proper horizontal or vertical start position relative to the target screen (black bars to the right, left, top, or bottom of the main viewport, or a distorted video).

### ***Sync Mouse, Single/Double Cursor***

These icons appear when the PS/2 mouse interface is active.

### ***Options***

The drop-down menu provides access to a number of options and features.

### ***Information Bar - Connection***

The left side of the information bar indicates whether the connection is encrypted (**Console (SSL)**) or unencrypted (**Console (Norm)**).

### ***Information Bar - Resolution***

Displays the horizontal by vertical resolution of the target system's video.

### ***Information Bar - Network Traffic***

Displays the approximate number of bytes per second incoming and outgoing to the window. An indication of the number of frames per second (fps) updated is also displayed. Incoming data is generally comprised of video updates. Outgoing data is generally comprised of keystrokes and mouse movements. When the target screen is not changing, **In** should be low or zero. If not, click the auto-adjust button. The amount of network traffic is a function of the detail in the captured screen, the rate at which the screen is changing, and the video encoding settings.

### ***Concurrent Access State***

- ◆ One user is connected to the Remote Console
- ◆ Multiple users are connected to the Remote Console
- ◆ This user has exclusive access to the Remote Console. No other clients may access the target system until exclusive access is disabled.
- ◆ Another user has exclusive access to the Remote Console. No other clients may access the target system until exclusive access is disabled by that user, or until that user closes their Remote Console window.

### ***Monitor Only State***

The far right icon shows whether this client may interact or simply view the target computer.

- ◆ Monitor Only is disabled; keyboard and mouse may interact with the target.
- ◆ Monitor Only is enabled; this client is view-only.



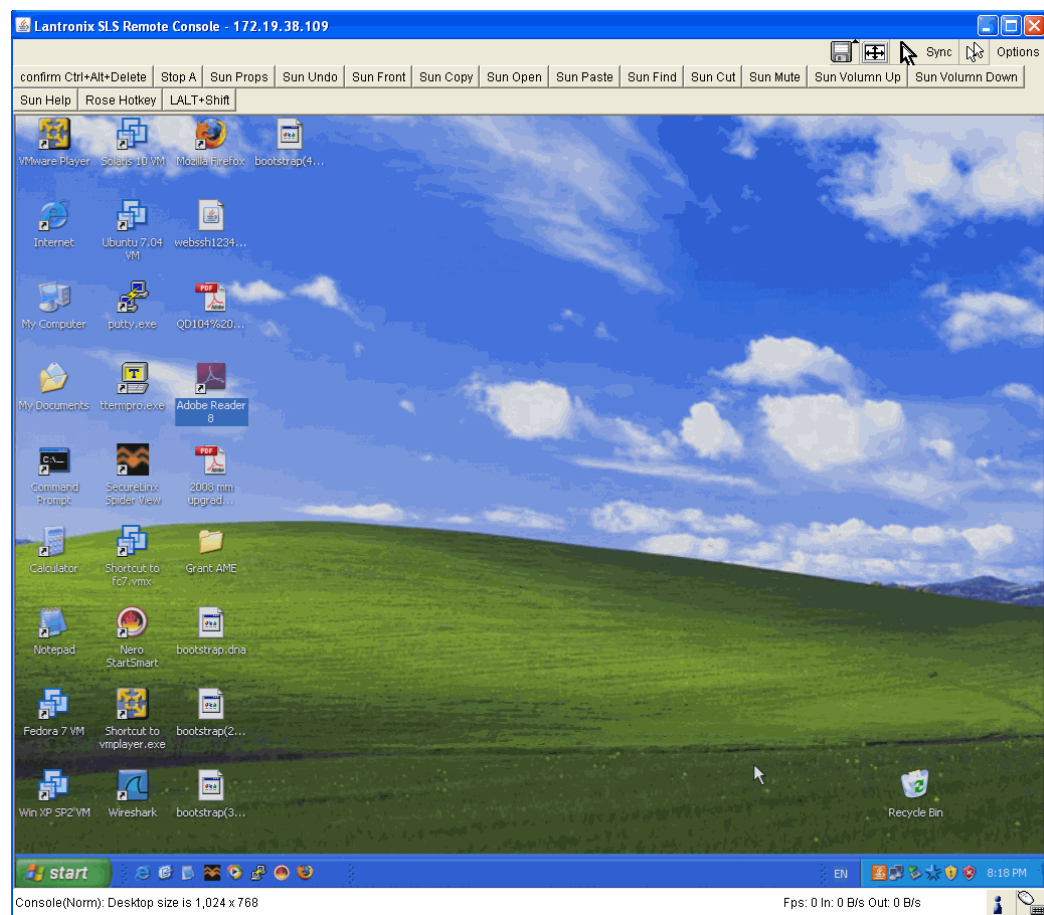
### Exclusive Access

- ◆ Only one user may access the Spider at a time.

### Basic Remote Console Operation

The “focus” of the client computer is the location of where the cursor is pointed. When the Remote Console window is open, there are three zones where the focus may be pointed:

1. Outside the Remote Console window, interaction is with the local computer's operating system or applications.
2. Inside the Remote Console window's viewport, interaction is with the target computer.
3. Inside the Remote Console window but outside the viewport, interaction is with the Remote Console control functions such as the toolbar or scroll bars.



Within the Remote Console viewport, interaction with the remote computer is generally the same as if there were a direct connection (with a minor lag due to network latency). Windows may be opened, applications run, settings changed, maintenance functions performed, even system reboots performed. Powering down the target computer results in powering down the Spider as well (unless the redundant supply is used).

## Mouse/Cursor Synchronization and Operation

Typically, mouse to cursor synchronization is an issue with digital KVM interfaces. Use of the USB mouse interface solves the problem, however many systems rely on a PS/2 interface. Spider provides several methods to fix the de-synchronization of local and remote cursors.

### Auto Video Adjustment

The left side of the target computer's screen must be aligned with the left side of the Remote Console viewport and that the tops align as well. If not, the local and remote cursors will always have a fixed offset of that amount, even if the USB interface is used. Clicking the **Auto Video Adjustment** one or more times typically cures any offset.

### Fast Sync and Intelligent Sync

The Spider uses two different algorithms for re-synchronizing local and remote cursors. Use the Fast Sync button on the toolbar to correct a fixed skew.

Intelligent Sync uses a different algorithm and is useful when the mouse settings have changed on the remote system or when Fast Sync does not work. It is accessed through the **Options→Mouse Handling** drop-down menu. The Sync button on the toolbar usually performs a Fast Sync, but will perform an Intelligent Sync if the video format has recently changed.

### Single and Double Mouse Modes

Continuous synchronization of local and remote cursors may not be feasible. The Spider provides a mode where only one cursor is visible when operating in the active Remote Console viewport. Click the **Single/Double** button on the toolbar to activate Single Mouse Mode. This is indicated by a single arrow in the **Single/Double** button. When in this mode, the Java KVM console “grabs” the local cursor after clicking within the viewport and will not release it until a “release-cursor” hot key sequence is given (**Alt+F12** by default). As there is only one cursor, and that one is confined to the active viewport, there is no issue with local to remote cursor tracking. There also is no local cursor; **Alt+F12** is required to free the cursor to move the focus from the active viewport. Clicking when the local cursor is within the viewport will re-grab the cursor. Single Mouse Mode may be exited by clicking on the **Single/Double** button.

If at some point the cursor seems to disappear, click **Alt+F12** or check the Single/Double Button as Single Mouse Mode may have been entered in error.

**Note:** Single Mouse Mode requires Sun Java 1.4 or higher

### Local Cursor

The Spider has an option to change the appearance of the local cursor when the focus is on the remote computer. Select **Options → Local Cursor** and select one of the following cursor options:

- ◆ Default: the local cursor maintains its appearance regardless of the focus location
- ◆ Transparent: the local cursor is invisible when the focus is on the remote computer. This is similar to Single Mouse Mode except the cursor is not “grabbed” and will reappear when moved outside of the active viewport.
- ◆ The other selections provide a change of appearance for a visual clue that the focus is on the remote computer; the cursor changes back when the focus is

back at the client system (including those areas of the Remote Console window outside the main viewport.)

Selections made in the Local Cursor submenu are associated with the current user and will be saved for the next Remote Console session.

## Optimizing Video

### *Auto and Manual Video Adjustment*

The Spider automatically recognizes and adapts to many standard video formats. (The complete list is in Appendix C.) When it first enters the Remote Console window, it recognizes and locks onto the video in order to provide a picture as soon as possible. Once within the window, click the **Auto Video Adjustment** button once or twice to provide a greater degree of optimization. The Auto Adjustment process analyzes the timing of the incoming video's horizontal and vertical sync signals then adjusts the digitizing hardware parameters. If there is slightly nonstandard timing, these parameters may be manually fine-tuned.

If it is necessary to adjust video hardware parameters, this may be done from **Options → Video Settings**. This brings up a window with a number of slider bars.

Adjust the brightness and contrast of the Remote Client window as presented by the Auto Adjustment. This is a hardware parameter and applies to all Spider users. Overall brightness and the contrast levels of each of the red, green, and blue primaries may be modified up or down. The Remote Console window immediately reflects the change. Once there is a satisfactory color-mapping, click **Save Changes** to retain those colors permanently for that video format. To discard the changes made, click **Undo Changes**. To return a particular setting or all settings to the original factory defaults, click **Reset this Mode** or **Reset All Modes**.

### **Clock and Phase**

The A/D converter uses these low-level settings in the digitization process. Adjustment should not be required unless advised by Lantronix Tech Support.

If the timing of the video signal is slightly off, the Auto Adjustment may not capture the frame at the right point. This will result in black bars along left, right, top, or bottom of the Remote Console viewport, and cutting off the opposite side of the captured image. The Offset sliders can be used to align the sides properly. Once there is correct alignment, click **Save Changes** to retain those settings permanently. To discard the changes made, click **Undo Changes**. To return a particular setting or all settings to the original factory defaults, click **Reset this Mode** or **Reset All**.

### *Video Encoding*

Various video encoding schemes have been defined to try to tailor the bandwidth usage to what is available. In addition to the predefined schemes, compression levels, and color depth can be manually adjusted. The default settings for each user are established in the **KVM Settings→User Console→Transmission Encoding** web page. To change the settings during a session, select **Options→Encoding→Predefined**, **Encoding→Compression**, **Encoding→Color Depth**, and **Encoding→Lossy** manual adjustments. These settings will be lost when the Remote Console window is closed; for nonvolatile changes use the **KVM Settings→User Console→Transmission Encoding** web page.

## Scaling Target Video to Client Resolution

In addition to the 1:1 pixel mapping mode, which is the default when the Remote Console window is first launched, scaling factors may be applied to the captured video in order to match various sizes of windows on the client. This scaling may be a fixed ratio or dynamically adjustable, as selected from the **Options→Scaling** selection. 100% is the default; it may result in a viewport smaller than the virtual screen and is moved around with scroll bars. 25% and 50% selections are optimal for viewing several target systems concurrently.

## Keyboard Functions

The Spider provides a number of useful functions for mapping or translating between the local keyboard/keycodes and the emulated keyboard presented to the target computer.

### *Soft Keyboard*

With remote control of a computer, it may be that the target system and client system are in different countries, using different languages. By using a Soft Keyboard, the local user can have the keycodes available to send to the target that are not on the local keyboard, without worrying about OS and application character set mappings.

Select **Options→Soft Keyboard→Mapping** to get a submenu listing the languages supported. Make the desired selection, and then verify it with **Show soft keyboard**.

Select **Options→Soft Keyboard→Show**. This provides an image of the currently selected Soft Keyboard. The Soft Keyboard sends single keystrokes as well as combinations of keys such as **Ctrl+C**. For a single keystroke, click on the button with the desired character. Single keys such as alphanumeric characters and punctuation are sent immediately. Special keys such as **Ctrl**, **Shift**, and **F1** to **F12** must be selected twice. The first click sends the signal “key is clicked.” The second click indicates the signal “key is released” to the remote system. After the first click the button will change its color to indicate that the key remains clicked, and that a code has not been sent. After the second click the button will appear as usual, showing that the keycode was sent.

Click the **Close** button on the title bar to close the soft keyboard.

### *Local Keyboard*

The Java Virtual Machine running the Remote Console applet on the client computer determines its keyboard language mapping automatically from the operating environment. There may be circumstances where it is unable to do so, such as when the keyboard mapping and OS language do not match. The **Options→Local Keyboard** selection allows manual designation of the language/layout of the keyboard on the client system.

### *Hotkeys*

Hotkeys provide an alternative method for sending keycode sequences defined in the section on Remote Console Button Keys. Click **Options→Hotkeys** and select the Button Key to be sent. If that Button Key has been defined with “Confirm”, a confirmation dialog box pops up before the keycode is sent.

## Other Remote Console Functions

### *Monitor Only*

When **Options→Monitor Only** is checked, the keyboard and mouse are disabled for this Remote Console window. The Monitor Only state is shown in the lower right corner of the Remote Console status bar. The user must have the appropriate permissions to change this setting.

### *Exclusive Access*

When **Options→Exclusive Access** is checked, no other client may open a Remote Console window to this Spider. Any open Remote Console windows on other clients will be disconnected. The Exclusive Access state is shown in the lower right corner of the Remote Console status bar. The user must have the appropriate permissions to change this setting.

### *Screenshot to Clipboard*

**Options→Screenshot** captures a snapshot of the entire target system's virtual screen to the clipboard for pasting into other applications.

### *Refresh Video*

The entire Remote Console viewport area is redrawn when the Remote Console window is first opened, and when the **Auto Adjust Video** button is clicked. As the encoding settings and noise filter may sometimes result in visible compression artifacts, selecting **Options→Refresh Video** can be used to redraw the entire viewport area.

## Telnet/SSH

In addition to interacting with the target system using the KVM Console, the Spider also allows text communication with the target via the Telnet Console, also a Java program window. Telnet and SSH are network protocols that enable a tunnel from the client system to the Spider's serial port. Once set up, it may be accessed through the web interface at the Telnet Console window, or using a Telnet/SSH client to connect directly. Note that Telnet/SSH cannot be used to connect to the Spider itself in order to control it, as the Spider has an HTTP and not a command line interface.

The Telnet Console is a Java program and has the same Java Runtime Environment requirements as the Remote Console. When the Telnet Console window is open, the user at the client system can send and receive characters directly to the serial port.

### Set up and Enable

To use Telnet or SSH, the serial port must be put in passthrough mode with the appropriate connection parameters and cabling with Telnet and/or SSH access allowed. If desired, the TCP port numbers also may be changed from their defaults. A user attempting to connect via Telnet or SSH must also have the appropriate permissions.

### Passthrough Use

When using Telnet/SSH in passthrough mode, the Spider just acts as a conduit for the serial data traveling between the client system and whatever is connected to the serial

port. This may be a COM port on the remote computer, or a serially controlled power strip, or anything else with an RS-232 port.

1. From the client system, use a Telnet or SSH utility to connect to the IP address of the Spider, at the assigned Telnet TCP port number.
2. The Spider will present **LOGIN** and **PASSWORD** prompts. Enter a valid user name and password. The user must have permissions set to use Telnet or SSH.
3. The Spider will reply with a Welcome and status, followed by a command line prompt. Selections are:
  - ◆ **Help** – displays a list of commands
  - ◆ **Version** – displays the current Spider firmware version number
  - ◆ **Terminal** – enter passthrough to serial port mode
  - ◆ **Logout** – terminates the Telnet or SSH connection
4. Enter **terminal** or **t** to open the connection to the serial port.
5. You are now connected and may interact with the attached serial console. Keystrokes are not locally echoed and must be echoed by the connected serial device.
6. Use the SSH or Telnet ability to send and receive serial data between the client and the serial port. The Spider does not echo this data back to the client.
7. When complete, enter **Esc-Exit** to return to the command line.
8. Enter **logout** or **l** to close the connection.

## Telnet Console Use

When using the Telnet Console, the Spider opens a window on the client system that provides direct access to the Telnet/SSH command line. This eliminates the need to have a Telnet or SSH utility running on the client system.

1. Click the **Terminal** button at the top of the Spider page. The user must have permissions set to use Telnet or SSH. The JRE will launch, and the Telnet Console window appears. Telnet Console and Remote KVM Console windows may be open concurrently.

```

Telnet to 172.19.208.2
Edit Terminal Help

Login: sysadmin
Password:

Welcome to the Lantronix SLS
Firmware: version 020119, build 6243
Last login: Wed Apr 23 19:31:11 2008 from 172.19.100.53
Current time: Wed Apr 23 19:31:40 2008
For a list of commands, type 'help'
[sysadmin@172.19.208.2]> help
SLS Command Line Help
-----
For more information on a command, type 'help <command>'
For example, 'help show history'.
For general CLI help, type 'help command line'.

set          sshkey|history|network
show         sshkey|history|network
connect      serial
admin        version|config
logout       terminates CLI session
[sysadmin@172.19.208.2]>

```

2. The Spider will present **LOGIN** and **PASSWORD** prompts. Enter a valid user name and password.
3. The Spider will reply with a Welcome and status, followed by a command line prompt. From the command line selections are:
  - ◆ **Help** – displays a list of commands
  - ◆ **Version** – displays the current Spider firmware version number
  - ◆ **Terminal** – enter passthrough to serial port mode
  - ◆ **Logout** – terminates the Telnet or SSH connection
4. Enter **terminal** or **t** to open the connection to the serial port.
5. Send and receive serial data between the Telnet Console window and the serial port. When in terminal mode, the Spider does not echo any characters typed back to the Telnet Console window, it simply passes them through to the serial port. Characters coming in from the serial port are displayed in the window.
6. When through, enter **Esc-Exit** to return to the command line.
7. Enter **logout** or **l** to close the connection.



## 6: Interfaces

The Interfaces tab provides pages for configuring network, serial port, KVM Console, Keyboard/Mouse, Video, and Virtual Media settings.

### Network Settings

Network settings may be found on the web page Interfaces→Network. As you are already talking to the Spider over a network, do not forget that changing the settings may result in dropping the connection. This will happen when you click the **Save** button. Take particular care to ensure your new settings are correct when making changes from a remote site!

**To configure network settings:**

1. Click **Interfaces→Network**. The **Network Settings** page displays.

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes links for KVM Console, Terminal, and Logout. The main navigation bar shows the current page is Network Settings. The page is divided into three main sections: Network Basic Settings, Network Miscellaneous Settings, and LAN Interface Settings. The Network Basic Settings section includes fields for IP auto configuration (None), Host name (lyonspider77), IP address (172.18.21.77), Subnet mask (255.255.0.0), Gateway IP address (172.18.0.1), Primary DNS server IP address (172.18.0.11), and Secondary DNS server IP address (172.18.0.13). The Network Miscellaneous Settings section includes fields for Remote Console & HTTPS port (443), HTTP port (80), TELNET port (23), SSH port (22), Bandwidth Limit (kbit/s), and checkboxes for Enable TELNET access, Enable SSH access, Disable Setup Protocol, and Enable remote console proxy access. The LAN Interface Settings section includes fields for Current LAN interface parameters (autonegotiation on, 100 Mbps, full duplex, link ok), LAN interface speed (Autodetect), and LAN interface duplex mode (Autodetect). At the bottom of the form, there are buttons for Save, Reset to defaults, and Reset. A status bar at the bottom of the page indicates the current version (02.01.16) and uptime (9 days, 20 hours, 45 minutes).

2. View or modify the following fields:

**Note:** A small green square to the right of a field name indicates that the current value is the default.



**Network Basic Settings**

<b>IP auto configuration</b>	Select <b>DHCP</b> or <b>BOOTP</b> to fetch network settings from the appropriate type of server. Select <b>NONE</b> for a fixed IP address.
<b>Host name</b>	DHCP servers can register a name for this Spider to assist in finding it, or you can configure it with a short host name or a fully qualified domain name.
<b>IP address</b>	If you are using a fixed IP address, enter it in the usual dot notation.
<b>Subnet Mask</b>	If you are using a fixed IP address, enter the subnet mask of the local network.
<b>Gateway IP address (optional)</b>	If the Spider is to be accessible from outside the local subnet, enter the IP address of the router providing access.
<b>Primary DNS Server IP Address (optional)</b>	For name resolution, enter the IP address of the primary Domain Name Server. This is optional, but needed if names rather than static IP addresses are used for certain Spider functions requiring network connections.
<b>Secondary DNS Server IP Address (optional)</b>	Enter the IP address of the Domain Name Server to be used if the Primary DNS Server cannot be reached.

**LAN Interface Settings**

<b>Current LAN interface parameters</b>	Displays current LAN interface settings.
<b>LAN interface speed</b>	Manual setup may be required for older equipment. With autonegotiation on, the window displays the current state of the link. Note that the parameters of the second Ethernet port are not configurable, they remain at autonegotiate. Select the speed from the drop-down menu.
<b>LAN interface duplex mode</b>	Select the duplex mode from the drop-down menu.

**Miscellaneous Network Settings**

<b>Remote Console &amp; HTTPS port</b>	Port number at which the Spider's Remote Console server and HTTPS server are listening. The default is 443.
<b>HTTP port</b>	Port number at which the Spider's HTTP server is listening. The default is 80.
<b>TELNET port</b>	Port number at which the Spider's Telnet server is listening. The default is 23.
<b>SSH port</b>	Port number at which the Spider's SSH server is listening. The default is 22.
<b>Bandwidth Limit</b>	The maximum network traffic generated through the Spider's primary Ethernet port, in kilobits. If left blank, there is no bandwidth limitation applied.
<b>Enable TELNET/SSH access</b>	For security, the default is having Telnet and SSH disabled. Check the appropriate box (es) and set up the serial port for Telnet/SSH to use the Telnet console.
<b>Disable Setup Protocol</b>	Spider View uses a special protocol to locate and set up Spider IP addresses. As a security measure you may wish to disable this protocol when deploying Spiders. If the protocol is disabled, Detector and the Spider network will not find the Spider.

<b>Enable remote console proxy access</b>	Enable the Java KVM console program to use a proxy server to connect to the Spider. You will most likely need to enable the program if you configure your web browser to use a proxy server to connect Spider web page.
<b>Proxy host</b>	<a href="#">Enter the proxy server's address.</a>
<b>Proxy port</b>	<a href="#">Enter the proxy port number.</a>

- Do one of the following:
  - Click **Save** to save settings.
  - Click **Reset to Defaults** to restore system defaults.
  - Click **Reset** to restore original settings.

## Serial Port Settings

After using the serial port to set up the Spider's network parameters, you may put the serial port to another use. You may establish A PPP connection to use a modem or other serial connection to log in to and operate the Spider. If you want to use the serial port to tunnel through to the network side of the Spider, Telnet and/or SSH connections are available.

**To configure the serial port:**

- Click **Interfaces**→**Serial Port**. The Serial Port Settings page displays.

The screenshot shows the 'Serial Port Settings' page in the Spider LANTRONIX web interface. The page has a navigation bar with 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'Serial Port' tab is selected. The settings are organized into three sections: 'Configuration login', 'Modem', and 'Passthrough access to serial port 1 via Telnet/SSH'. The 'Passthrough' section is active, showing fields for Speed (9600), Data bits (8), Parity (none), Stop Bits (1), and Handshake (None). There are also buttons for 'Save', 'Reset to defaults', and 'Reset'. The footer includes copyright information and version details.

- Modify the following fields:

<b>Configuration Login</b>	Select this option to use the serial port locally only to set up network parameters or reset the unit.
<b>Modem</b>	Connect to the Spider with a dial-up or ISDN connection, using PPP. Essentially, the Spider acts as an ISP that you dial in to. The client system will need to be set up accordingly, for example using the Windows Network Connection Wizard. Change the following

	<p>parameters as necessary:</p> <p><b>Serial Line Speed:</b> Most modems support 115200 bps.</p> <p><b>Modem Init String:</b> The initialization string sent out to set up the modem. If you have a special modem or are going through a PBX requiring an access sequence, you may modify the string. Consult the modem's manual on the AT command syntax.</p> <p><b>Modem server IP addresses:</b> As part of the PPP handshake, IP addresses are assigned to the remote device.</p> <p><b>Modem client IP address:</b> IP address assigned to the Spider.</p>
<b>Passthrough Access to serial port 1 via Telnet/SSH</b>	<p>The serial port may be used to connect to the target server's COM port for integrated access to command line functions or used to control a serial-interfaced peripheral. Telnet and SSH are network protocols that enable a tunnel from the client system over the network to the Spider's serial port. Once the port is set up, it may be accessed through the web interface at the Telnet Console window, or using a Telnet/SSH client to connect directly.</p> <p>Set the following parameters to match connected equipment:</p> <p><b>Speed:</b> The speed with which the device port exchanges data with the attached serial device.</p> <p>From the drop-down list, select the baud rate. Most devices use 9600 for the administration port, so the device port defaults to this value. Check the equipment settings and documentation for the proper baud rate.</p> <p><b>Data bits:</b> Number of data bits used to transmit a character. From the drop-down list, select the number of data bits. The default is <b>8</b> data bits.</p> <p><b>Parity:</b> Parity checking is a rudimentary method of detecting simple, single-bit errors. From the drop-down list, select the parity. The default is <b>none</b>.</p> <p><b>Stop Bits:</b> The number of stop bit(s) used to indicate that a byte of data has been transmitted. From the drop-down list, select the number of stop bits. The default is <b>1</b>.</p> <p><b>Handshake:</b> A method of preventing buffer overflow and loss of data. The available methods include none, software (xon/xoff), and hardware (RTS/CTS). The default is <b>none</b>.</p>

3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## KVM Console Settings

### User Console

The Remote Console window into the target system has settings that may be changed for the way each individual user interacts with the Spider. When a user is created by copying from an existing user, the Remote Console settings will be copied as well. You can change these settings on the **Interfaces→KVM Console Settings** page. Note that if you

are using the Spider View application, these settings do not apply; see the Spider View User Guide for further information.

The way in which the Spider transmits video data back to the client system can be tailored for the type of network connection. On a LAN where bandwidth is not an issue, compression is not required and the speed of updates can be maximized. For other connections, the optimum user interaction needs to trade off image quality and update speed to fit the size of the pipe. Because various users may be accessing the Spider over different connections, these parameters are applied on a user-by-user basis. The default is set for maximum image quality and speed of updates, which results in high data rate and hence is suitable for LANs where bursts of up to 2 Mbytes/second are acceptable.

### To modify the user console:

1. Click **Interfaces→KVM Console**. The **Remote Console Settings for User** page displays.

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes links for Interfaces, User Accounts, Services, and Maintenance. The main content area is titled "KVM Console Settings" and is for user "sysadmin". It contains several sections:

- Transmission Encoding:** Includes radio buttons for Automatic Detection, Pre-configured (selected), and Manually. Under Pre-configured, there are dropdowns for Network speed (LAN (high color)), Compression (0 - none), and Color depth (16 bit - high color).
- KVM Console Type:** Includes radio buttons for Default Java VM (selected) and Sun Microsystems Java Browser Plugin. A note states: "If your system doesn't have the Java Plugin, this option will download 11MB Plugin for extended KVM Console function."
- KVM Console Deployment:** Includes radio buttons for Java Web Start (selected) and Applet.
- Miscellaneous KVM Console Settings:** Includes checkboxes for Start in Monitor Mode and Start in Exclusive Access Mode.
- Mouse Hotkey:** Includes a text field for Hotkey (Help) set to Alt+F12. A note states: "Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode)."
- KVM Console Virtual Keys:** A table with 20 rows, each with a Key Definition (Help) and a Name. Key 1 is set to "confirm Ctrl+Alt+Delete" and Key 2 is set to "ctrl+alt+f1" with Name "Linux CLI". Key 3 is set to "alt+f7" with Name "Linux GUI".

At the bottom, there are buttons for Save, Reset to defaults, and Reset. A status message indicates "Stored value is equal to the default." The footer shows copyright information and version details.

2. Configure the following settings:

**KVM Console Settings for User**

<b>&lt;User drop-down menu&gt;</b>	Select the user from the drop-down menu. The settings on this page apply only to the selected user. When a user is created by copying from an existing user, the KVM Console Settings will be copied as well.
------------------------------------	---

**Transmission Encoding**

<b>Automatic Detection</b>	This option uses an algorithm to try to determine what sort of connection is being used, and sets up parameters to match. These settings may change from login to login depending on the state of the network at that point.
<b>Preconfigured</b>	Establishes a set of parameters optimized for each of a number of connection types. The default transmission encoding is LAN (high color), which is uncompressed with a 16 bit color depth. Other data networks may be chosen from the list, and the compression and color depth will be configured accordingly. Network speed?
<b>Manual</b>	Allows the direct control of the compression factor and color depth. The simplest way to reduce bandwidth is to cut the color depth down to 8 bits; subtle color shades will be gone but the overall image is very usable. Dialing up the compression level also makes available even further reductions in color depth, all the way down to black and white (1 bit.) As compression level increases and/or color depth decreases, image quality and responsiveness to changes deteriorates but required bandwidth is reduced.

**KVM Console Type**

<b>Default Java VM</b>	Select this option to use Java on the client system launching the applet. If no Java environment is installed, the console window will not launch. The default is enabled.
<b>Sun Microsystems Java Browser Plugin</b>	Force the system to use the platform-independent Sun version instead when launching the Remote Console applet.

**KVM Console Deployment**

**Note:** Users have two ways to deploy the Remote Console program. Both provide same functionalities; however, technically the way to deploy the program on a client machine is different.

The default is Java Web Start. Applet deployment is available in case the user cannot connect via Java Web Start. This usually should not happen unless the user has a special proxy server or firewall that blocks Java Web Start.

<b>Java Web Start</b>	Select this option to use Java Web Start deployment method.
<b>Applet</b>	Select this option to use the Applet deployment method.

**Miscellaneous KVM Console Settings**

<b>Start in Monitor Mode</b>	Results in the Remote Console window being view-only when launched for this user. This may be changed to interactive mode from within the Remote Console window, if the user has appropriate permission.
<b>Start in Exclusive</b>	Upon any subsequent launch of the Remote Console applet by the

<b>Access Mode</b>	selected user, terminates any other users' Remote Console windows and locks out any other users trying to access the Remote Console window. This may be changed from within the Remote Console window to allow shared access, if the user has appropriate permission.
--------------------	---

### Mouse Hotkey

<b>Hotkey (Help)</b>	When the Remote Console window is open, a key code that is not captured by the client system is needed for certain mouse functions. The default is <b>Alt+F12</b> . Change the key code if necessary.
----------------------	---

### KVM Console Virtual Keys

<b>Key Definition (Help)</b>	<p>Button keys allow simulating keystrokes at the remote system that cannot be generated from the client keyboard. A flexible syntax allows for combinations of keys being clicked in combination or in sequence, with optional pauses and an optional confirmation-before-sending dialog box.</p> <p>One key is predefined, for <b>Ctrl+Alt+Delete</b> (with confirmation.) The syntax to define a new Button Key is as follows:</p> <p><b>&lt;keycode&gt;[+ -]&gt;[*]&lt;keycode&gt;]*</b></p> <p>Keycode is the key to send. Multiple key codes are concatenated with a + or a - sign. The + sign builds key combinations, all keys will be clicked until a - sign or the end of the combination is encountered. All clicked keys will be released in reversed sequence. The - sign builds single, separate key clicks and key releases.</p> <p><b>Note:</b> For a list of keys and further explanation, click the <b>Help</b> link at the top of the <b>Key Definition</b> column.</p>
<b>Name</b>	Enter the name to appear on the button in the Remote Console window. Up to nine Button Keys may be defined for each user.

3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Keyboard/Mouse

To modify the keyboard and mouse settings:

1. Click **Interfaces**→**Keyboard/Mouse**. The **Keyboard/Mouse Settings** page displays.

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes links for **Interfaces**, **User Accounts**, **Services**, and **Maintenance**. The **Interfaces** tab is selected, and the **Keyboard/Mouse** sub-tab is active. The page title is **Keyboard/Mouse Settings**. The settings are organized into a form with the following fields and options:

- Host Interface:** A dropdown menu set to **Auto**. A green status icon and the text "active: USB" are shown.
- Force USB Full Speed Mode:** A checkbox that is checked. Below it, a note states: "Some host machine do not support negotiable speed in the BIOS. Enable this when host machine does not detect keyboard/mouse in the BIOS."
- Keyboard Model:** A dropdown menu set to **Generic 104-Key PC**.
- Key release timeout:** A checkbox that is unchecked.
- Timeout after:** A dropdown menu set to **100 msec**. Below it, a note states: "Enable key release timeout if you experience duplicated keystrokes during poor network performance."
- Country Code:** A checkbox that is checked.
- Country:** A dropdown menu set to **English (US)**. Below it, a note states: "Enable if host machine requires keyboard to send a country code in order to use certain language. Most OS does not require this except Sun Solaris."
- USB Mouse Type:** A dropdown menu set to **Other Operating Systems**.
- Mouse speed:** Three radio buttons: **Auto** (unchecked), **Fixed scaling : 1.00** (checked), and **Absolute mouse scaling for Mac server** (unchecked).

At the bottom of the form, there is a green status icon and the text "Stored value is equal to the default." Below this are three buttons: **Save**, **Reset to defaults**, and **Reset**.

The footer of the page includes the copyright notice "© 2007-2008 Lantronix, Inc.", navigation links for **Home**, **KVM Console**, **Terminal**, and **Logout**, and the version number "Version 02.01.16 (V2.1RC16\_2008-04-01)".

2. Modify the following fields:

### Keyboard/Mouse Settings

<b>Host Interface</b>	<p>In general, the USB interface is preferred because it provides superior mouse tracking. The <b>Host Interface</b> drop-down provides three selections.</p> <p>In the default mode, <b>Auto</b>, the Spider will attempt to determine whether the attached computer supports a USB keyboard/mouse. If it does, that interface will be activated, but if it does not, the Spider will fall back to PS/2. If you have a USB model Spider and the attached computer does not support USB, you will have a view-only system.</p> <p>On the PS/2 model Spider, select <b>PS/2</b> to force the PS/2 interface or <b>USB</b> to require USB. This selection has no effect on the USB model Spider.</p>
<b>Force USB Full Speed Mode</b>	Some older systems do not support USB high-speed mode and may not recognize the keyboard/mouse. Enable this option for Spider to negotiate in USB full speed mode.

### Keyboard Model

<b>&lt;PS/2 keyboard model drop-down menu&gt;</b>	<p>When operating in PS/2 interface mode, key codes from several layouts may be emulated.</p> <p><b>Generic 104-key PC</b> for the traditional layout.</p> <p><b>Generic 109-key PC</b> for keyboard with added Windows keys. (Use 109 for Japanese keyboard.)</p> <p><b>Apple Macintosh</b> for Mac layout.</p> <p><b>SUN Type 6</b> for Sun Solaris layout.</p>
---	---

### Key Release Timeout

<b>Key release timeout</b>	Network delays may sometimes result in duplicated keystrokes. Enable Key Release Timeout to fix this problem.
<b>Timeout after</b>	Enter time, in msec.

### Country Code

<b>Country Code</b>	Select the check box to enable the Spider to recognize the country code. Enable if the host machine requires the keyboard to send a country code to use a certain language. Most operating systems do not require this except Sun Solaris.
<b>Country</b>	From the drop-down list, select the code of the desired country.

### USB Mouse Type

<b>&lt;USB mouse type drop-down menu&gt;</b>	Different operating systems running on the target system require different mouse emulation protocols. One selection is available for newer versions of Windows and Mac OS/X, and another for <b>Other Operating Systems</b> (e.g., Linux).
--	--



### Mouse Speed

<b>Mouse speed</b>	<p>Select the method of assigning mouse speed.</p> <p><b>Auto</b> mouse speed determines the speed and acceleration settings of the target system. It is the recommended setting for most applications.</p> <p><b>Fixed scaling</b> translates a one-pixel motion on the client system to a selectable number of pixels moved on the target system. As the 1 to n mapping is linear, this will only work when there is no compression acceleration or other special effects turned on at the target system.</p>
--------------------	---

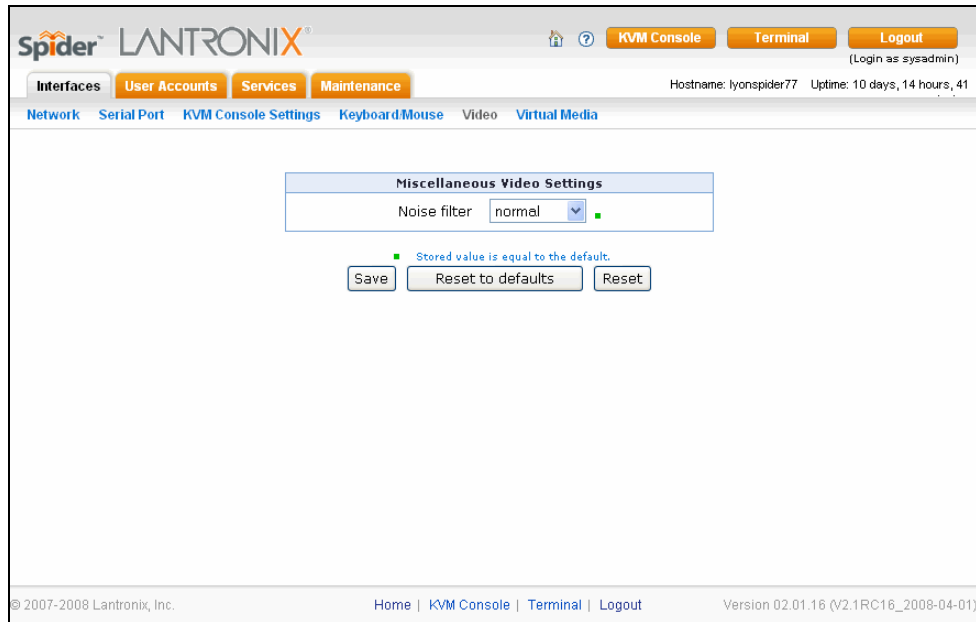
3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Video

The Spider works by capturing and digitizing the analog video coming from the attached computer. This analog video may have more or less low-level electrical noise present, depending on the nature of the video card or embedded video controller. When viewed on a monitor, this noise (if random) is invisible as the display is being redrawn 60 to 100 times a second. Inside the Spider, however, the algorithm sees that noise as something changing on the screen, so that requires sending off an update to the client system. This can result in a constant stream of data even when the image on the target computer's screen is not moving. In order to avoid this, at **Interface→Video→Miscellaneous Video Settings** the Spider has a selection for noise filter. The larger filter openings will filter out more of the noise, at the cost of potentially missing small incremental changes and seeing some compression artifacts (blocky-ness). Filter settings of **Normal** or **Large** will work for most applications. Be sure to try the Remote Console Auto Adjust Video button a few times before deciding that a constant stream of data represents electrical noise requiring a larger filter setting.

#### To modify video settings:

1. Click **Interfaces→Video**. The **Miscellaneous Video Settings** page displays.



2. Select the **Noise Filter** level from the drop-down menu.
3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Virtual Media

The Spider provides a powerful capability called Virtual Media (or Virtual Disk). Using the USB port, the Spider can present either a local floppy disk image or a redirected remote CD-ROM image to the target computer. This can allow system recovery in conditions as bad as having local disks down and no primary network connection. With Floppy Disk Image, the user can upload an image to the Spider's memory, which then emulates a locally attached floppy drive. With CD-ROM Image, a Windows or other SAMBA share can emulate a locally attached CD-ROM, for instance to update software.

Drive Redirection allows you to share (redirect) your local drive (floppy drives, hard disks, CD ROMs and other removable devices like USB sticks) with the remote system over a TCP network connection. Thus, with Drive Redirection, you can use a virtual disk drive on the remote computer instead of an image file. It is also possible to enable a remote machine to write data to your local disc.

### Notes:

- ◆ Drive Redirection supports only Windows as the client computer since it redirects based on a drive letter.
- ◆ See [Appendix B: Virtual Media Example](#) for a complete demonstration of how to use Virtual Media.

**To open the Virtual Media page:**

1. Click **Interfaces**→**Virtual Media**.

Spider LANTRONIX

KVM Console Terminal Logout (Login as sysadmin)

Interfaces User Accounts Services Maintenance Hostname: sls-sunset3 Uptime: 0 days 2 hours 40 minutes

Network Serial Port KVM Console Settings Keyboard/Mouse Video Virtual Media

**Virtual Media**

Image file set successfully

**Virtual Media Active Image**

**CD-ROM Image**

Share Host/IP: 172.19.39.23  
Share Name: images  
Image File with Path: ubuntu-8.04-desktop-i386.iso  
User Name: \*\*\*\*\*  
Password: \*\*\*\*\*

Reactivate Unset

**Image on Windows Share**

This allows you to share a CD-ROM/DVD image (e.g. example.iso) over a Windows Share with a maximum size of 4.7GB. This image will be emulated to the host as USB device.

Share Host/IP: 172.19.39.23  
Share Name: images  
Image File with Path: ubuntu-8.04-desktop-i386.iso  
User Name (optional):  
Password (optional):

Set Reset

**Virtual Media Options**

**Drive Redirection**

Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.

☐ Disable Drive Redirection  
☒ Force read-only connections

**Virtual Media Options**

☐ Disable USB Mass Storage if no image is loaded  
Stored value is equal to the default.

Save Reset to defaults Reset

**Floppy Image Upload**

This allows you to upload a binary image (e.g. example.img) with a maximum size of 1.44MB to the Lantronix SLS. This image will be emulated to the host as USB device.

Floppy Image File:  Browse...

You must remove the current virtual disk to install a floppy image.

© 2007-2008 Lantronix, Inc. Home | KVM Console | Terminal | Logout Version 04.01.00 (Devel)

The functions of the Virtual Media page are discussed below.

### To prepare for drive redirection:

1. Enter the following:

### Virtual Media Active Image

<b>Virtual Media Active Image</b>	Once you set <b>Image on Windows Share</b> or <b>Floppy Image File</b> (on this web page), information about the currently assigned (active) image displays.
-----------------------------------	--

### Drive Redirection

<b>Disable Drive Redirection</b>	Drive Redirection is enabled by default. Select this checkbox to disable the ability to share the local drive with the remote system.
<b>Force read-only connections</b>	Select to prevent the remote drive from writing to your local drive. Selected by default.  <b>Warning:</b> Clearing the <b>Force read-only connections</b> check box may result in file system errors and data corruption because of drive caching when data is written back to the Redirected local drive.

### Virtual Media Options

The operating system on the target computer must have a USB mass storage driver installed in order to use Virtual Media. As the BIOS on some systems does not always

support mass storage emulation on the USB interface, the system default is to disable USB mass storage unless an image is loaded. This option may be unselected to use

<b>Disable USB Mass Storage</b>	Select the checkbox to disable USB mass storage if no image is loaded. Selected by default.  Clear the check box if an image is loaded.
<b>Force read-only connections</b>	Select to prevent the remote drive from writing to your local drive. Selected by default.  <b>Warning:</b> Clearing the <b>Force read-only connections</b> check box may result in file system errors and data corruption because of drive caching when data is written back to the Redirected local drive.

2. Do one of the following:

- ◆ Click **Save** to save settings.
- ◆ Click **Reset to Defaults** to restore system defaults.
- ◆ Click **Reset** to restore original settings.

### Image on Windows Share

In this section of the page, you can enable the Spider to access a CD-ROM image up to 4.7 GB on a Windows shared folder via SAMBA. The Spider then makes that image accessible to the target computer by emulating a USB disk drive.

**Note:** Windows 2003 and Windows Vista do not support this feature.

Appropriate administrative permissions to access the host and file are needed, as well as the ability to see that computer over the network from the Spider.

The connection remains mounted until the current user logs out or the Spider is rebooted. Other client systems logging into the Spider will see the active image in all Virtual Media pages.

### To share a CD-ROM image:

1. Enter the following:

<b>Share Host/IP</b>	IP address of the host of the Windows shared folder.
<b>Share Name</b>	Name of the host of the Windows shared folder.
<b>Image File with Path</b>	Name and path to the CD-ROM image. (The file must be structured as a CD-ROM image.) The filename appears as the <b>Active Image</b> and the image is available to the target computer as a letter drive (e.g., <b>F:</b> ).
<b>User Name</b> (optional)	User name for accessing the host and file.
<b>Password</b> (optional)	Password for accessing the host and file.

2. Do one of the following:

- ◆ To discard your changes, click **Reset**.

- ◆ To mount the image, click **Set**. Information about the image displays in the **Virtual Media Active Image** section of the page and the CD icon displays on the remote console.

The screenshot shows the Spider LANTRONIX web interface. At the top, there are tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. Below these are sub-tabs for 'Network', 'Serial Port', 'KVM Console Settings', 'Keyboard/Mouse', 'Video', and 'Virtual Media'. The 'Virtual Media' sub-tab is selected. The main content area is titled 'Virtual Media' and contains a message 'Image file set successfully'. It is divided into three main sections: 'Virtual Media Active Image', 'Image on Windows Share', and 'Floppy Image Upload'. The 'Virtual Media Active Image' section has fields for 'Share Host/IP' (172.19.39.23), 'Share Name' (images), 'Image File with Path' (FC3-i386-DVD.iso), 'User Name' (test1), and 'Password' (\*\*\*\*\*). It includes 'Reactivate' and 'Unset' buttons. The 'Image on Windows Share' section has similar fields and 'Set' and 'Reset' buttons. The 'Floppy Image Upload' section has a 'Floppy Image File' field with a 'Browse...' button and a message: 'You must remove the current virtual disk to install a floppy image.' Below the 'Virtual Media Active Image' section is the 'Virtual Media Options' section, which includes 'Drive Redirection' (with a checkbox for 'Disable Drive Redirection' and a checked checkbox for 'Force read-only connections') and 'Virtual Media Options' (with a checked checkbox for 'Disable USB Mass Storage if no image is loaded' and a note 'Stored value is equal to the default'). There are 'Save', 'Reset to defaults', and 'Reset' buttons at the bottom of the options section.

3. If desired, in the **Virtual Media Active Image** section:

- ◆ Click **Reactivate** if the remote console does not recognize the image.
- ◆ Click **Unset** to remove the current image file. (This option is available only when a user uploads a floppy image.)
- ◆ Click **Download** to save the image file.

### Floppy Image

In the **Floppy Image Upload** section, you can upload a floppy disk image to the Spider, which then appears to the attached computer as a physical floppy drive. The desired floppy image file will be uploaded from the client system or from a network drive accessible to the client system. The file must be structured as a floppy image. To make a floppy image, search for and use a utility such as `dd` or `rawwrite`. The maximum image size is 1.44 MB. For larger images, use the CD-ROM Image function.

The image file remains in Spider until the current user logs out, or the Spider is rebooted. Other client systems logging into the Spider will also see the active image in all Virtual Media pages.

#### To upload a floppy image file:

1. In the **Floppy Image Upload** section (bottom right), click **Browse** to locate the floppy image file.
2. Do one of the following:
  - ◆ Click **Reset** to discard your changes.

- Click **Upload** to load the image into Spider's memory. This floppy drive is accessible to the remote computer as a letter-name floppy drive (e.g., **B:**). Information about the image displays in the **Virtual Media Active Image** section of the page.

The screenshot shows the Spider LANTRONIX web interface. At the top, there are navigation tabs: Interfaces, User Accounts, Services, and Maintenance. Below these are sub-tabs: Network, Serial Port, KVM Console Settings, Keyboard/Mouse, Video, and Virtual Media. The 'Virtual Media' sub-tab is active. The main content area is titled 'Virtual Media' and contains a message: 'Floppy image uploaded successfully.' Below this message are three main sections: 'Virtual Media Active Image', 'Image on Windows Share', and 'Floppy Image Upload'. The 'Virtual Media Active Image' section shows 'Floppy Image' with 'Image Name: floppy.img' and buttons for 'Reactivate', 'Download', and 'Discard'. The 'Image on Windows Share' section has fields for 'Share Host/IP', 'Share Name', 'Image File with Path', 'User Name (optional)', and 'Password (optional)', along with a note: 'You must remove the current virtual disk to install a CD-ROM image.' The 'Floppy Image Upload' section has a 'Floppy Image File' field with a 'Browse...' button and a note: 'You must remove the current virtual disk to install a floppy image.' There are also 'Virtual Media Options' with checkboxes for 'Disable Drive Redirection' (unchecked), 'Force read-only connections' (checked), and 'Disable USB Mass Storage if no image is loaded' (checked). A 'Save' button is at the bottom of this section.


- If desired, in the **Virtual Media Active Image** section:

- Click **Reactivate** if the remote machine does not recognize the image.
- Click **Download** to save the image file.
- Click **Discard** to remove the current image file.

## Connecting to a Redirected Drive

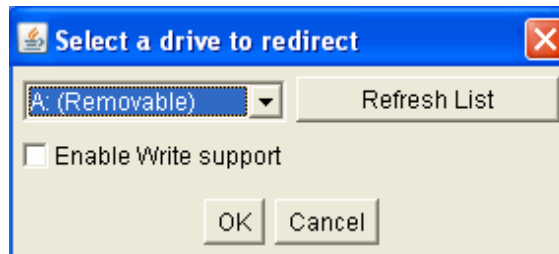
### To connect to a redirected drive:

If **Drive Redirection** is enabled, you can connect to the drive. Depending on the combination of the type of drive and the **Force read-only connections** setting, different warnings display.

- Click the **KVM Console** button at the top of the Spider web page or click the console image that you see when you log in to the Spider. The Remote Console displays?
- Click the disk icon  in the toolbar. Drive Redirection buttons display at the top left of the page.

The screenshot shows a toolbar titled 'Drive Redirection'. It contains three buttons: 'Connect Drive', 'Connect ISO', and 'Disconnect'. To the right of these buttons is a status indicator that says 'Not connected'. Below the buttons, it says 'Drive Redirection disconnected.'

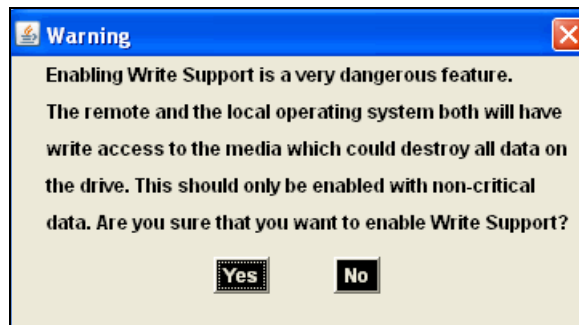
- Click the **Connect Drive** button at the top of the page. The **Select a drive to redirect** dialog box opens.



4. From the drop-down list, select the drive you want to redirect.

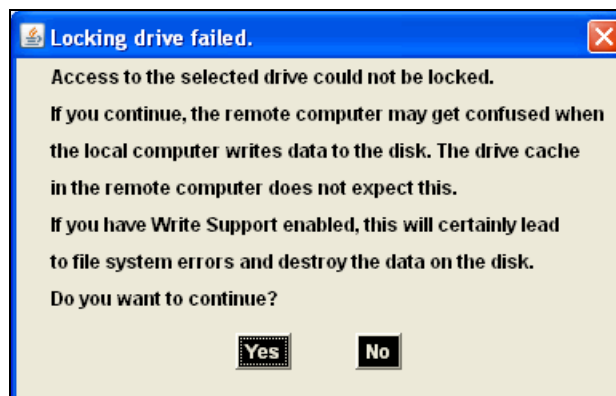
**Note:** To refresh the list after adding or removing a drive, click the **Refresh List** button.

5. If desired, select the **Enable Write support** check box.
6. Click **OK**. Depending on your selections, the following events or warnings display:
  - ◆ If you select **Enable Write support**, the following warning displays:



Because of the danger of destroying all data on the drive, click **Yes** only if you are certain of what you are doing.

- ◆ If you select the hard disk from the drop-down list, the following warning may display:



When drive redirection is enabled and a connection is made, the Spider attempts to lock the locally shared drive. This prevents local access to the drive while it is being shared with the remote PC. If the drive cannot be locked, and write capability is enabled, the local computer can be exposed to file corruption if both the local and remote computers attempt to write to the local drive at the same time. In general, the Spider cannot lock the boot partition (typically the C: drive) because locking would prevent the OS from accessing necessary files. We

recommend that you use drive redirection with a non-boot partition or with a separate physical drive like a second hard drive, external storage device, or CD/DVD drive.

- ◆ If you select a drive other than the hard disk, and do not select **Enable Write support**, the connection to the redirection of the drive is successful.

**Note:** *Appendix B: Virtual Media Example provides a complete demonstration of how to use Virtual Media.*



## 7: User Accounts

### Local vs. Remote Authentication

User names and groups may be administered on the Spider to allow varying levels of access and control to different classes of users. To log in to the Spider, a user must be authenticated by means of a password. This authentication may take place locally, where the user name and associated password are stored in the Spider's memory. The Spider may query a centralized database using RADIUS or LDAP to determine if a given user may log in. In both of these cases, the user name must be defined on the Spider where it has its permissions assigned.


### Local User Management

On a Spider, each user name has settings and permissions associated with it. Settings affect how the user interfaces with the Remote Console. Permissions allow or forbid the user from performing various actions on the Spider's web pages. A newly assigned user has permissions inherited from an assigned group, if any, or individual permissions if no group is assigned.

### Modifying Passwords

To change current user password:

1. Click **User Accounts**→**Change Password**. The Change Password page displays.



The screenshot displays the Spider LANTRONIX web interface. At the top, there is a navigation bar with tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'User Accounts' tab is selected. Below this, there is a sub-navigation bar with links for 'Change Password', 'User/Group', 'Permissions', and 'Authentication'. The 'Change Password' link is active. The main content area shows a 'Change Password' form with three input fields: 'Old Password', 'New Password', and 'Confirm New Password'. Below the form are 'Save' and 'Reset' buttons. The top right of the interface shows 'KVM Console', 'Terminal', and 'Logout' buttons, along with the text '(Login as sysadmin)'. The bottom of the interface shows the hostname 'lyonspider77', uptime '10 days, 14 hours, 52', and version '02.01.16 (V2.1RC16\_2008-04-01)'.

2. Enter the current password under **Old Password**.
3. Enter the new password under **New Password** and **Confirm New Password**.
4. Click **Save** to save your settings, or click **Reset** to restore original settings.

## User and Group Management

You must be logged in under a user name that has permissions for User/Group Management to access this page. The Spider supports a maximum of 50 configured users. When defining a user, make sure the group to which the user will belong has already been created.

To configure users and groups:

1. Click **User Accounts** → **User/Group**. The **User/Group Management** page displays.

To configure a user:

1. Configure the following fields:

### User Management

<b>Existing users</b>	To modify or copy an existing user, select that user from the drop-down menu and click <b>Lookup</b> .
<b>New user name</b>	Enter the new user's name. Minimum 1 character.
<b>Full user name</b>	Enter the full name of the configured user. Minimum 1 character.
<b>Password</b>	Enter the password for the user. Minimum 4 characters.
<b>Confirm Password</b>	Re-enter the password for the user.
<b>Email address</b>	(Optional) Enter the user's email address.
<b>Mobile number</b>	(Optional) Enter the user's mobile phone number.

<b>Group Membership</b>	Select the user's group from the drop-down menu.
<b>Enforce user to change password on next login</b>	Select checkbox to require the user to change the password upon initial login.

2. Do one of the following:

- ◆ Click **Create** to add the new user.
- ◆ Click **Modify** to change an existing user.
- ◆ Click **Copy** to create a new user based on the selected existing user.
- ◆ Click **Delete** to delete an existing user.
- ◆ Click **Reset** to restore original settings.

**To configure a user group:**

1. Configure the following fields:

### Group Management

<b>Existing Groups</b>	To copy or modify a group, select the group from the drop-down menu. Click <b>Lookup</b> .
<b>New Group Name</b>	Enter the new group's name.

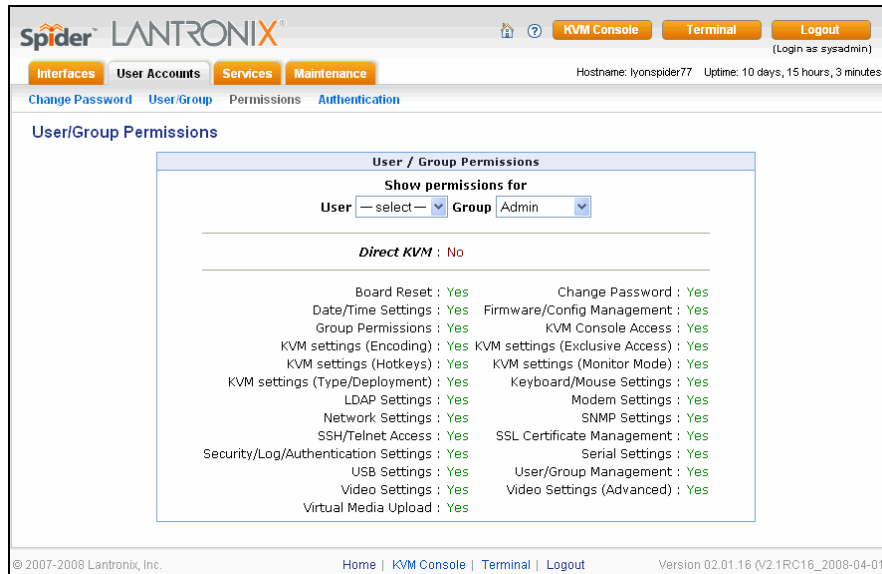
2. Do one of the following:

- ◆ Click **Create** to add the new group.
- ◆ Click **Modify** to change an existing group.
- ◆ Click **Copy** to create a new group based on the selected existing group.
- ◆ Click **Delete** to delete an existing group.
- ◆ Click **Reset** to restore original settings.

## User Permissions

**To modify user permissions:**

1. Click **User Accounts→Permissions**. The **User/Group Permissions** page displays.



2. From the drop-down menu, select a **User** or **Group** to configure:
  - ◆ If you created a user belonging to a group, and you want to change permissions for the group, select **Group**.
  - ◆ If you created a user who does not belong to any group, then select **User**.
3. From the **Direct KVM** drop-down menu, do one of the following:
  - ◆ Select **Yes** to enable the user or group to access the Remote Console only. After a user is authenticated, it launches the Java KVM console program.
  - ◆ Select **No** (default) to display the web page after login.
 

**Note:** Setting **Yes** may overwrite some selected permissions selected in step 4.
4. Modify the displayed permissions as necessary for the selection.
5. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Remote Authentication

If the Spider's Authentication Settings have been set to Local Authentication (the default), the Spider uses its own database to perform authentication. If one of the remote authentication protocols is selected, the Spider communicates with a remote server to authenticate user passwords.

**To configure authentication settings:**

1. Click **User Accounts**→**Authentication**. The Authentication Settings page displays.

**Authentication Settings**

☒ Local Authentication ☐ LDAP

LDAP Server IP

LDAP Server Base DN

LDAP Server Type

User Search Sub-filter

Bind Name

Bind Password

Confirm Bind Password

☐ RADIUS

	Server	Shared Secret	Auth. Port	Acc. Port	Timeout	Retries
1.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text" value="1812"/>	<input type="text" value="1813"/>	<input type="text" value="1"/>	<input type="text" value="3"/>

Individual remote users must be added to the Spider account prior to the Spider allowing remote users (LDAP, RADIUS) access.

2. Modify the following fields:

**Local Authentication**

When Local Authentication is selected, the Spider will authenticate against its internal database of users and passwords, as described in Local User Management.

**LDAP**

When you select LDAP Authentication, the Spider will communicate with a Microsoft Active Directory or generic LDAP server for user authentication. The user profile must be set up in the local database as described in Local User Management, but no password is stored locally. When a user attempts to log in, the Spider contacts the specified LDAP server, which will either approve or denies access.

<b>LDAP Server IP</b>	Enter the name or IP address of the LDAP server, reachable over the network by the Spider, containing the user database. Be sure to configure a DNS server if a name rather than address is used.
<b>LDAP Server Base DN</b>	Specify the Distinguished Name (DN) where the directory tree starts in the user LDAP server.
<b>LDAP Server Type</b>	Select the type of the external LDAP server. Available selections are <b>Generic LDAP</b> and <b>Microsoft Active Directory</b> . If a Generic LDAP Server is selected, edit the LDAP scheme.
<b>User Search Sub-filter</b>	Select to restrict the search for users by adding an additional search filter to each query for a user.
<b>Bind Name</b>	The name for a non-anonymous bind to an LDAP server. This item has the same format as LDAP Base. One example is cn=administrator,cn=Users,dc=domain,dc=com.
<b>Bind Password and Confirm Password</b>	Password for a non-anonymous bind. This entry is optional. Acceptable characters are <b>a-z</b> , <b>A-Z</b> , and <b>0-9</b> . The maximum length is 127 characters.

## RADIUS

When RADIUS is selected, the Spider communicates with a RADIUS server for user authentication. To access a Spider set up for RADIUS, log in with a name and password. The Spider contacts the RADIUS server for authentication and, if approved, the Spider uses the locally stored user profile. If there is no such profile access via RADIUS will be refused. The RADIUS implementation also has a timeout whereby if there is no activity for half an hour the connection to the Spider will be terminated.

<b>Server</b>	Enter the name or IP address of the RADIUS server, reachable over the network by the Spider, containing the user database. Configure a DNS server if a name rather than an address is used.
<b>Shared Secret</b>	A shared secret is a text string that serves as a password between the RADIUS client and RADIUS server. In this case the Spider acts as a RADIUS client. A shared secret is used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret and to verify that the RADIUS message has not been modified in transit (message integrity). Enter a maximum of 128 alphanumeric characters and symbols such as an exclamation point ("!") or an asterisk ("*").
<b>Authentication Port</b>	The port the RADIUS server listens for authentication requests. The default value is <b>1812</b> .
<b>Accounting Port</b>	The port the RADIUS server listens for accounting requests. The default value is <b>1813</b> .
<b>Timeout</b>	Sets the request time-to-live in seconds. The time-to-live is the time to wait for the completion of the authentication request. If the request job is not completed within this interval of time it is cancelled. The default value is <b>1</b> second.
<b>Retries</b>	Sets the number of retries if a request could not be completed. The default value is <b>3</b> times.

3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## 8: Services

### Date/Time

The Spider contains an internal real time clock that maintains a basic date and time after being set. The clock, however, will reset if the unit loses power. If an accurate date and time are critical, the Spider supports synchronization with Network Time Protocol servers. Internally, the date and time are only used to timestamp events in the log and for the inactivity timeout.

**To configure the date and time settings:**

1. Click **Services**→**Date/Time**. The **Date/Time Settings** page displays.

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'Services' tab is active, and the 'Date/Time' sub-tab is selected. The 'Date/Time Settings' form is displayed with the following fields:

- UTC Offset: +/- 0 h
- User specified time (selected):
  - Date: 1 / 11 / 1970 (mm/dd/yyyy)
  - Time: 18 : 59 : 33 (hh:mm:ss)
- Synchronize with NTP Server (unselected):
  - Primary Time server: [empty field]
  - Secondary Time server: [empty field]

Buttons at the bottom: Save, Reset to defaults, Reset. A status message indicates 'Stored value is equal to the default.'

2. Modify the following fields:

<b>UTC Offset</b>	Time servers deliver time as Coordinated Universal Time (UTC, or Greenwich Mean Time). Select the appropriate offset in hours $\pm$ from the drop-down menu.
<b>User Specified Time</b>	Manually input the current date and time. The Spider keeps time as long as power is applied. It has an internal calendar, but does not know about daylight savings time and requires resetting twice a year. The internal clock accuracy is $\pm 30$ ppm.
<b>Synchronize with NTP Server</b>	Enter a primary and secondary time server in the respective fields. Ensure NAT and firewalls are set up to allow the protocol to pass. Also, provide the Spider with DNS server names.

3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Security

General settings for security parameters such as encryption and access control are at **Services→Security**. Other areas with security implications include User Management/Permissions, Authentication, Network Settings, and the Event Log; see the appropriate sections for information on those areas.

### To modify security settings:

1. Click **Services→Security**. The **Security** page displays.

**Spider LANTRONIX**

Hostname: Spider-WinXP-VM Uptime: 1 days, 13 hours, 10

**Security Settings**

**HTTP Encryption**

☐ Force HTTPS for Web access

**Login Limitations**

☐ Enable Single Login Limitation

**KVM Encryption**

KVM Encryption ☒ Off ☐ Try ☐ Force

**Authentication Limitation**

☒ Enable Screenshot Access without Authentication  
Screenshot is accessible at 'http(s):(Spider IP Address)/screenshot.jpg'

☒ Enable **Direct KVM** Console Access without Authentication  
Enable this option to launch KVM Console by 'http(s):(Spider IP Address)'.

**Group based System Access Control**

Please note: 'Save' is required, or changes will be lost.

☒ Enable Group based System Access Control

Default Action:

Rule #	Starting IP	Ending IP	Group	Action
1	0.0.0.0	255.255.255.255	All	ACCEPT
2	172.19.39.20	172.19.39.20	Admin	ACCEPT
3	172.19.39.21	172.19.39.21	Admin	ACCEPT
4	172.19.39.22	172.19.39.22	Admin	ACCEPT
5	172.19.39.24	172.19.39.24	@spider_nogroup2	ACCEPT

Admin

Append Insert Replace Delete

☒ Stored value is equal to the default.

Save Reset to defaults Reset

© 2007-2008 Lantronix, Inc. Home | KVM Console | Terminal | Logout Version 02.01.19 (V2.1RC19\_2008-04-15)

2. Modify the following fields:

### HTTP Encryption

#### Force HTTPS for Web Access

Typically, the Spider listens on both HTTP and HTTPS ports for incoming connections. If this box is checked, access can only be made using SSL, and connection requests on the HTTP port will be ignored. See the section on Certificate for further information on how the Spider identifies itself using a cryptographic certificate.



**Login Limitations**

<b>Enable Single Login Limitation</b>	If this box is checked, each username may only have one logged in connection at a time. If unchecked, multiple instances of username logins are allowed.
---------------------------------------	--

**KVM Encryption**

<b>KVM Encryption</b>	<p>In addition to the SSL encryption of the Spider's web pages, the keyboard, mouse, and video data may be encrypted. Select <b>Off</b> to use no encryption.</p> <p>Select <b>Try</b> for the Spider to attempt to make an encrypted connection but will back off to unencrypted if one cannot be established.</p> <p>Select <b>Force</b> for an encrypted connection to be made, or an error will be reported.</p>
-----------------------	--

**Group Based System Access Control**

<b>Enable Group Based System Access Control</b>	When this box is checked, the rules for IP based access are enforced. They are ignored when the box is not checked.
<b>Default Action</b>	If after evaluation of all rules a request for connection from a given IP address has not had either an <b>Accept</b> or <b>Drop</b> decision made, this selection can allow it to be either Accepted or Dropped. In other words, this drop-down defines the default action for IP addresses with no rules defined.
<b>Rule creation and editing</b>	<p>Spiders come from the factory with one rule defined as an example of the rule structure: Rule 1 allows all groups access from source IP 0.0.0.0 to 255.255.255.255. Additional rules may be entered in the edit boxes.</p> <p><b>Rule Number:</b> Defines where in the evaluation sequence this rule is to be applied.</p> <p><b>Starting and Ending IP Addresses:</b> Define the range over which the rule applies.</p> <p><b>Group:</b> Defines which user group is affected by this rule. Built-in groups include <b>Admin</b>, <b>All</b>, and <b>Unknown</b> (no group assigned). As additional groups are defined in <b>User Management</b>→<b>Users</b>→<b>Group Management</b>, they will appear in the drop-down. A rule can apply to only one group at a time.</p> <p><b>Action:</b> Chooses whether this is to be a <b>Drop</b> or <b>Accept</b> rule.</p> <p>After a rule has been defined, it needs to go in the correct place in the list.</p> <p><b>Append:</b> Puts the rule at the end of the list. The rule number changes to reflect the last position on the list.</p> <p><b>Insert:</b> Puts the rule in the place on the list indicated by the rule number, renumbering and moving down the other rules to make room.</p> <p><b>Replace:</b> Deletes the previous rule of that number and replaces it with the new rule.</p> <p><b>Delete:</b> Deletes the rule of that number and moves the others up. Note that for a <b>Delete</b>, the fields other than the rule number do not need to be filled in.</p>

### Authentication Limitation

<b>Enable Screenshot Access without Authentication</b>	Select this option when you need to access the snapshot image without logging in to the Spider. If enabled, the screenshot can be read directly with <code>http(s)://&lt;spiderIPAddress&gt;/screenshot.jpg</code> . One use of this unauthenticated screenshot is to read it from a Google gadget
<b>Enable Direct KVM Console Access without Authentication</b>	Select this option to launch the Remote Console without authentication by entering the Spider's IP address ( <code>http(s)://(Spider IP address)</code> ) in the browser's <b>Address</b> field or type <code>javaws http(s)://(Spider IP address)</code> in the command line.

3. Do one of the following:

- ◆ Click **Save** to save settings.
- ◆ Click **Reset to Defaults** to restore system defaults.
- ◆ Click **Reset** to restore original settings.

## Certificate

The Spider uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the Spider has to expose its identity to a client using a cryptographic certificate. Upon leaving the factory this certificate and the underlying secret key is the same for all Spiders and will not match the network configuration where it is installed. The certificate's underlying secret key is also used for securing the SSL handshake. Leaving the default certificate unmodified is all right in most circumstances and is necessary only if the network facility is vulnerable to man-in-the-middle attack.

It is possible to generate and install a new base64 x.509 certificate that is unique for a particular Spider. The Spider is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA).

#### To create and install an SSL certificate:

1. Click **Services→Certificate**. The Certificate Signing Request page displays.

The screenshot shows the Spider LANTRONIX web interface. At the top, there are navigation tabs: Interfaces, User Accounts, Services, and Maintenance. Below these are sub-tabs: Date/Time, Security, Certificate, Event Log, SNMP, and Spider Network. The main content area displays the 'Certificate Signing Request (CSR)' form. The form includes fields for Common name, Organizational unit, Organization, Locality/City, State/Province, Country (ISO code), Email, Challenge password, Confirm Challenge password, and Key length (bits). The Key length is set to 1024 bits. A 'Create' button is at the bottom of the form. The footer shows copyright information for Lantronix, Inc. and the version number 02.01.16 (V2.1RC16, 2008-04-01).

2. Modify the following fields:

<b>Common name</b>	The network name of the Spider once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the Spider with a web browser without the prefix http://. In case the name given here and the actual network name differ, the browser will pop up a security warning when the Spider is accessed using HTTPS.
<b>Organizational unit</b>	This field specifies to the department within an organization to which the Spider belongs.
<b>Organization</b>	The name of the organization to which the Spider belongs.
<b>Locality/City</b>	The city where the organization is located.
<b>State/Province</b>	The state or province where the organization is located.
<b>Country (ISO code)</b>	The country where the organization is located. This is the two-letter ISO code (e.g., US for the United States).
<b>Email</b>	The email address of a contact person responsible for the Spider and its security.
<b>Challenge password/Confirm Challenge password</b>	Certain certification authorities require a challenge password to authorize later changes on the certificate (e.g., revocation of the certificate). The minimal length of this password is four characters.
<b>Key length (bits)</b>	Select the key length from the drop-down menu.

- Click **Create** to initiate the Certificate Signing Request generation. Download the CSR by clicking **Download**. The **Download** button displays when a certificate is created. Send the saved CSR to a CA for certification.
- Click **Upload** to upload the certificate from the client computer to the Spider. The Spider now has its own certificate used for identifying itself to its clients.

## Event Log

The Event Log maintains a list of significant events locally. Alternatively it can use an NFS log file, SMTP email, or SNMP to distribute event information on the network. The Spider monitors five classes of events with the logging of each enabled or disabled.

To configure event log settings:

1. Click **Services**→**Event Log**. The **Event Log** page displays.

**Spider LANTRONIX**

Interfaces | User Accounts | **Services** | Maintenance

Date/Time | Security | Certificate | **Event Log** | SNMP | Spider Network

Hostname: Spider-VlnXP-VM Uptime: 1 days, 13 hours, 58 (Login as sysadmin)

### Event Log Settings

**Event Log Targets**

- ☒ List Logging Enabled
  - Entries shown per page: 35
  - Clear internal log: [Clear](#)
- ☒ NFS Logging Enabled
  - NFS Server: 172.19.39.20
  - NFS Share: /home/glenn/nfs1
  - NFS Log File: slsevlog
- ☐ SMTP Logging Enabled
  - SMTP Server:
  - Receiver Email Address:
  - Sender Email Address:
- ☒ SNMP Logging Enabled
  - Destination IP: 172.19.39.19
  - Community: CMNMPublic

[Click here to view the Lantronix SLS SNMP MIB](#)

**Event Log Assignments**

Event	List	NFS	SNMP
Board Message	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Remote Console	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Host Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Authentication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

☒ Stored value is equal to the default.

© 2007-2008 Lantronix, Inc. Home | KVM Console | Terminal | Logout Version 02.01.19 (V2.1RC19\_2008-04-15)

2. Modify the following fields:

### Event Log Targets

<b>List Logging Enabled</b>	Check this box to use the internal log list of the Spider. The maximum number of entries is 1,000. Every entry that exceeds this limit overrides the oldest one. The number of log entries shown on each page may be changed in the text box. The internal log list is cleared when power is removed from the Spider, or when you click the <b>Clear</b> button.
<b>NFS Logging Enabled</b>	The Spider can write log information to a file on an NFS server. Provide the name of the server, share, and file in the boxes. The NFS share will be mounted immediately, and an error message will result if it cannot be found.
<b>SMTP Logging enabled</b>	With this option, the Spider is able to send emails to an address given by the email address. These emails contain the same description strings as the internal log file and the mail subject contains the event class. To use this log destination, specify an <b>SMTP Server</b> , the <b>Receiver Email Address</b> , and <b>Sender Email Address</b> . Enter the mail server and SMTP port as <b>&lt;serverip&gt;:&lt;port&gt;</b> .

<b>SNMP Logging Enabled</b>	If selected, the Spider sends an SNMP trap to a specified destination IP address every time a log event occurs. Configure the <b>Destination IP</b> and <b>Community</b> . View the SNMP MIB implemented in the Spider by clicking on the <b>SLS SNMP MIB</b> link.
-----------------------------	---

### Event Log Assignments

<b>Event Log Assignments</b>	Select the event classes for monitoring, local logging, and exportation.
------------------------------	--

3. Do one of the following:

- ◆ Click **Save** to save settings.
- ◆ Click **Reset to Defaults** to restore system defaults.
- ◆ Click **Reset** to restore original settings.

## SNMP

The Spider has an internal SNMP agent that has various objects accessible in its MIB. It also can generate traps based on events. The Spider permits enabling or disabling the SNMP agent, input read and write communities, location information, contact information, and viewing the MIB.

**To configure SNMP settings:**

1. Click **Services**→**SNMP**. The **SNMP Settings** page displays.

The screenshot displays the 'SNMP Settings' page in the Spider LANTRONIX web interface. The page has a navigation bar with tabs for 'Interfaces', 'User Accounts', 'Services', and 'Maintenance'. The 'Services' tab is active, and the 'SNMP' sub-tab is selected. The main content area shows the 'SNMP Settings' form. The 'Enable SNMP Agent' checkbox is checked. Below it, there are fields for 'System Location' and 'System Contact' (set to 'Lantronix, Irvine, CA, USA'). The 'Use SNMPv3' section has radio buttons for 'DES Encryption' (set to 'Off') and 'Force'. There are also fields for 'Read Username', 'Read Password', 'Write Username', and 'Write Password'. The 'Use SNMPv1' section has radio buttons for 'Read Community' (set to 'public') and 'Write Community' (set to 'private'). At the bottom of the form, there is a link 'Click here to view the SNMP MIB'. Below the form, there are buttons for 'Save', 'Reset to defaults', and 'Reset'. A small green square icon indicates 'Stored value is equal to the default.' The footer of the page shows '© 2007-2008 Lantronix, Inc.', 'Home | KVM Console | Terminal | Logout', and 'Version 02.01.16 (V2.1RC16\_2008-04-01)'.

2. Modify the following fields:

<b>Enable SNMP Agent</b>	Click the checkbox to enable the Spider SNMP agent, and enter the system location and the contact name for the system.
--------------------------	--

<b>Use SNMPv3</b>	<p>Select to use SNMPv3 (rather than SNMPv1) and enter the following:</p> <p><b>DES Encryption:</b> Select whether to turn off or enable encryption with Data Encryption Standard (DES),</p> <p><b>Read Username:</b> User ID for a user with read-only authority to use to access SNMP v3.</p> <p><b>Read Password:</b> Password for a user with read-only authority to use to access SNMP v3. Up to 32 characters.</p> <p><b>Write Username:</b> Enter a user ID for users with read-write authority. Up to 32 characters.</p> <p><b>Write Password:</b> Enter a password for the user with read-write authority to use to access SNMP v3. Up to 20 characters.</p>
<b>Use SNMPv1</b>	<p>Select to use SNMPv1 (rather than SNMPv3) and enter the following:</p> <p><b>Read Community:</b> Enter the SNMP read community name. The default is <b>public</b>.</p> <p><b>Write Community:</b> Enter the SNMP write community name. The default is <b>private</b>.</p>

3. Do one of the following:
  - ◆ Click **Save** to save settings.
  - ◆ Click **Reset to Defaults** to restore system defaults.
  - ◆ Click **Reset** to restore original settings.

## Spider Network

The Spider Network option enables you to view the properties of the other Spiders on the network.

**Note:** The information shown on the web interface represents a snapshot in time. To see the most recent data, reload the web page.

### To view the Spider network:

1. Click **Services** → **Spider Network**. The Spider Network page displays.

Spider LANTRONIX®

[KVM Console](#)
[Terminal](#)
[Logout](#)
  
 (Login as: sysadmin)

[Interfaces](#)
[User Accounts](#)
[Services](#)
[Maintenance](#)

Hostname: lyonspider77 Uptime: 10 days, 20 hours, 52

[Date/Time](#)
[Security](#)
[Certificate](#)
[Event Log](#)
[SNMP](#)
 Spider Network

No.	IP/Web	Hostname	Direct KVM	Preview	Terminal	SSH	Telnet	MAC Address	Model	Ver.	Descr.	SN
1	172.18.2.219		N/A	N/A	N/A	No	No	00:80:A3:8C:00:23	USB	2.1	V2.1RC17_	008014000035
2	172.18.21.75		N/A	Preview	Terminal	Yes	Yes	00:20:4A:80:8C:0A	PS2	2.1	V2.1RC16_	002048447B1B
3	172.18.21.77	lyonspider77	N/A	N/A	Terminal	Yes	Yes	00:80:A3:DE:FA:CE	PS2	2.1	V2.1RC16_	0080EF44E10D
4	172.18.18.44		N/A	N/A	N/A	No	No	00:80:A3:8C:0D:DD	PS2	2.0		008033353439
5	172.18.11.18		N/A	N/A	Terminal	Yes	Yes	00:80:A3:8C:0F:B2	USB	2.1	V2.1B13_2	008014004018
6	172.18.2.220	ltxspider03	N/A	N/A	N/A	Yes	Yes	00:80:A3:8C:02:89	PS2	2.1	V2.1RC17_	008014000649
7	172.18.18.45		N/A	Preview	Terminal	Yes	Yes	00:80:A3:8C:1C:F9	PS2	2.1	V2.1RC16_	008014007417
8	172.18.2.218	ltxspider01	N/A	N/A	N/A	Yes	No	00:80:A3:8C:09:A9	USB	2.1	V2.1RC17_	008014002473

© 2007-2008 Lantronix, Inc.
 [Home](#) |
 [KVM Console](#) |
 [Terminal](#) |
 [Logout](#)
 Version 02.01.16 (V2.1RC16\_2008-04-01)

## 9: Maintenance

The administrator performs various maintenance activities on the Spider. These include viewing its status, back up and restore configuration files, update firmware, view the event log and reset the unit.

### Device Status

The Device Status page contains a table with information about the Spider's hardware and firmware. This information is useful if technical support is required.

**To view device information:**

1. Click **Maintenance**→**Device Status**. The Device Status page displays.

2. View or modify the following:

#### Device Information

Device Information	Displays hardware and software information.
--------------------	---

#### Connected Users

Connected Users	Displays the IP address of all connected users and their level of activity. It also shows whether the user is connected to the Remote Console, and if so, whether exclusive access mode is activated.
-----------------	---



## System Identifier

<b>ID indicator off</b>	Displays whether a Spider's LED is lit. Each Spider has an orange LED that can be lit by remote control, making it easier to locate. By default the LED is off, but you can clear the box to turn on the LED on the Spider.
-------------------------	---

## Style Sheet

<b>Style Sheet</b>	From the drop-down menu, select the color of the tabs and buttons at the top of the Spider pages. Orange is the default.
--------------------	--

- Do one of the following:
  - Click **Save** to save settings.
  - Click **Reset to Defaults** to restore system defaults.
  - Click **Reset** to restore original settings.

## Configuration

To update the configuration:

- Click **Maintenance** → **Config/Factory Defaults**. The following page displays:

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes links for Interfaces, User Accounts, Services, and Maintenance. The Maintenance section is active, showing options for Device Status, Config/Factory Defaults, Update Firmware, View Event Log, and Unit Reset. The main content area is divided into two panels: Configuration Backup and Configuration Restore. The Configuration Backup panel has a Backup button. The Configuration Restore panel has a Config File input field with a Browse... button, a checkbox for Preserve Basic Network Settings, a warning message, and an Upload/Restore button. The footer contains copyright information and version details.

- Select one of the following options:

<b>Configuration Backup</b>	To back up all settings to a file on the client system, click the <b>Backup</b> button, and save the file to the desired location. This is the file uploaded to the Spider upon system restore.
<b>Configuration Restore</b>	<p>To return the Spider settings to a previously saved configuration, browse to select the configuration file.</p> <p><b>Config File:</b> Browse to and select the backed up configuration file.</p> <p><b>Preserve Basic Network Settings:</b> Select this check box to preserve the current network basic settings on the Network</p>

	<p>Settings page and import only the remaining settings from the configuration file.</p> <p>Click the <b>Upload/Restore</b> button. If you select this option, the Spider reboots after you apply the update.</p>
<b>Factory Defaults</b>	<p>To restore factory settings, click the <b>Restore</b> button. The SLM reboots after you apply the update.</p> <p>To keep basic network settings rather than restoring defaults, select the <b>Preserve Network Settings</b> option in the Configuration Restore area.</p>

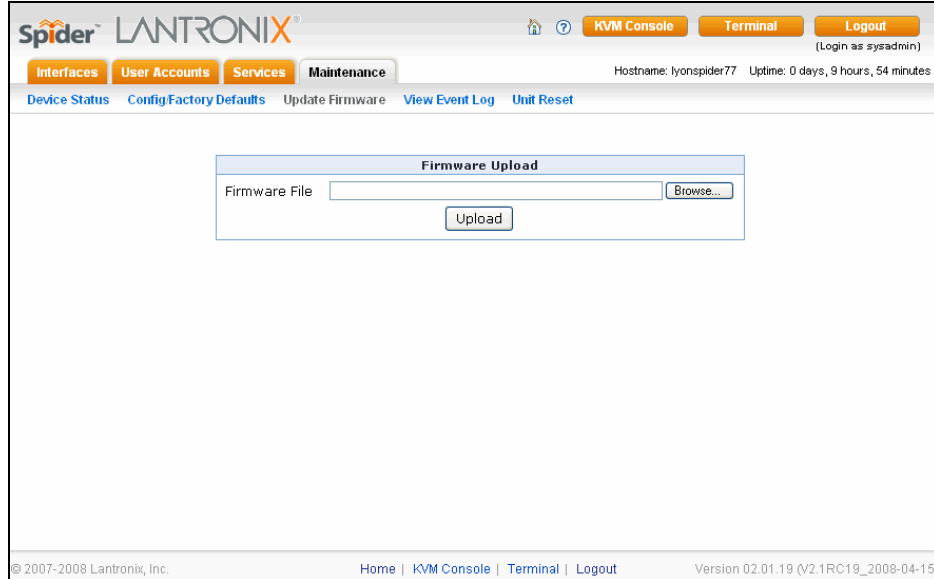
## Update Firmware

Many of the functions and features of the Spider are implemented in firmware and capable of field upgrades. The latest firmware may be found at [www.lantronix.com](http://www.lantronix.com). The firmware file, when uncompressed, is approximately 4 Mbytes in size and has a .bin suffix.

Upon updating firmware, the Spider resets itself. After the reset, the login page displays (if not, manually return to the login page).

### To update Spider firmware:

1. Download the firmware file to the client system's local drive or an accessible network drive.
2. Click **Maintenance**→**Update Firmware**. The **Firmware Upload** page displays.



3. Click **Browse**. In the pop-up window, navigate and locate the firmware file.
4. Click **Upload** to copy the file into the Spider's local memory. When uploaded correctly, the Firmware Upload window displays the version number of the new firmware. Click the **Update** button to replace the old with the new, or to cancel the operation, click the **Discard** button. Do not interrupt power to the Spider during the update process.

## View Event Log

To view the current event log:

1. Click **Maintenance**→**Event Log**. The **Event Log** page displays.

The screenshot shows the Spider LANTRONIX web interface. The top navigation bar includes links for KVM Console, Terminal, and Logout. Below this, a secondary navigation bar highlights the Maintenance section, which contains links for Device Status, ConfigFactory Defaults, Update Firmware, View Event Log, and Unit Reset. The View Event Log link is active, displaying the Event Log page. The page features a table with the following data:

Date	Event	Description
01/01/1970 10:05:26	Board Message	Uploaded firmware file discarded.
01/01/1970 10:04:21	Board Message	Firmware file uploaded by user 'sysadmin'. 02.00.00 (Build 5786).
01/01/1970 09:42:58	Authentication	User 'sysadmin' logged in from IP address 172.18.100.26
01/01/1970 08:40:03	Remote Console	Connection to client 172.18.100.26 closed.
01/01/1970 08:40:00	Remote Console	Connection to client 172.18.100.26 established.
01/01/1970 08:39:28	Authentication	User 'sysadmin' logged in from IP address 172.18.100.26
01/01/1970 00:00:57	Board Message	Device successfully started.
01/15/1970 05:13:48	Board Message	Firmware updated to 02.01.19 (Build 6243). There were errors!
01/15/1970 05:13:01	Board Message	Firmware file uploaded by user 'sysadmin'. 02.01.19 (Build 6243).
01/15/1970 05:12:48	Authentication	User 'sysadmin' logged in from IP address 172.19.211.19
01/15/1970 04:50:11	Authentication	User 'sysadmin' logged in from IP address 172.19.211.19
01/12/1970 21:19:31	Authentication	User " failed to log in from IP address 172.18.100.26
01/12/1970 21:19:30	Authentication	User " failed to log in from IP address 172.18.100.26
01/12/1970 21:19:30	Authentication	User " failed to log in from IP address 172.18.100.26
01/12/1970 21:19:30	Authentication	User " failed to log in from IP address 172.18.100.26
01/12/1970 20:15:21	Remote Console	Connection to client 172.18.0.65 closed.
01/12/1970 20:15:21	Remote Console	Connection to client 172.18.0.65 established.
01/12/1970 20:12:49	Authentication	User 'sysadmin' logged in from IP address 172.18.0.65
01/12/1970 19:32:01	Authentication	User 'sysadmin' logged in from IP address 172.20.192.104

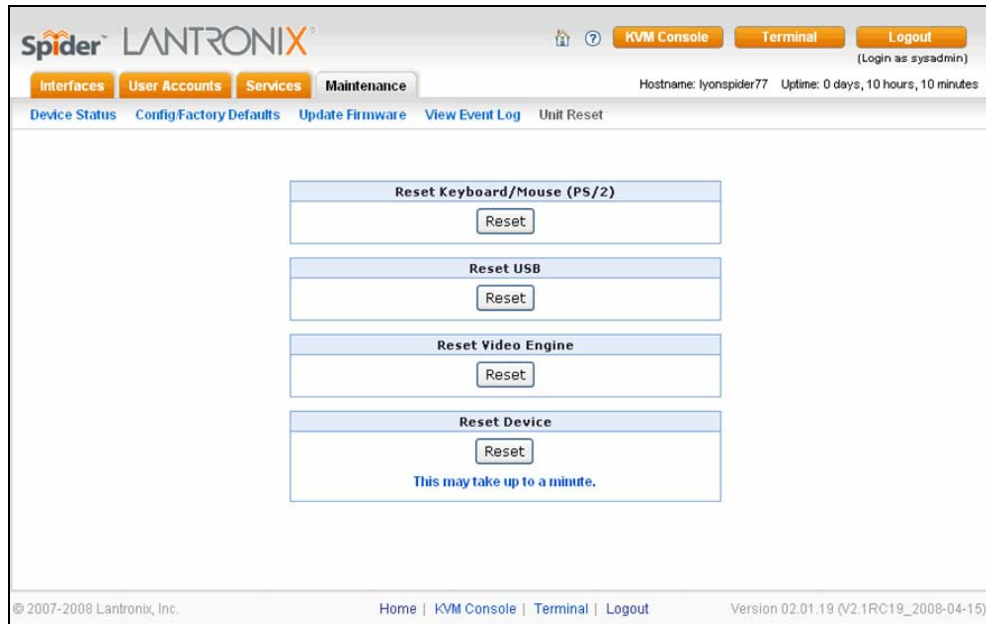
Navigate between logs by clicking **Prev** and **Next**.

## Unit Reset

In general, the Spider requires a reset when implementing a firmware update. In the event of an abnormal operation, a number of subsystems may be reset without resetting the entire Spider.

To reset the Spider:

1. Log into the Spider as **sysadmin**.
2. Click **Maintenance**→**Unit Reset**. The following page displays.



3. Click the **Reset** button for **Reset Keyboard/Mouse (PS/2)**, **Reset USB**, or **Reset Video Engine** to clear and reset the subsystem. Resetting subsystems does not terminate connected users.
4. To perform a complete reset, click **Reset Device**. A prompt requesting confirmation displays. A complete reset closes all user connections and performs a full reboot.

## iGoogle Gadgets

You can create an iGoogle gadget that enables you to view and access multiple Spiders on one web page. You access a snapshot of each of the Spider's Remote Console without logging in to the Spider.

Anyone with a Google email account (gmail.com) can create an iGoogle gadget for viewing web pages. There are two types of iGoogle gadgets: public gadgets and private gadgets. When you submit a gadget's XML code to Google, it becomes part of the iGoogle public gadgets, which are listed for import on iGoogle web pages. When a gadget's XML code is stored on a private server, the gadget stays private and is usable only by users who are aware of its location.

### To use iGoogle gadget to manage multiple spiders:

1. Click **Services**→**Security**.
2. In the Authentication Limitation section, select the **Enable Screenshot Access without Authentication** check box.
3. Edit a file similar to the example below and save it with extension ".xml." This example assumes the file is saved as **spider1.xml**. The sample code displays a snapshot and refreshes the image every minute. Also, clicking the snapshot opens the remote console program or spider web page, depending on your settings.

```
<?xml version="1.0" encoding="UTF-8" ?>
<Module>
  <ModulePrefs title="Spider Preview (Your Spider IP Address)"
```

```

height="240" scaling="false" />
<Content type="html">
<![CDATA[
<center>
<div>

</div>
<script>
var c = 0
var t
function updateSpiderSnapshot()
{
    document.getElementById('sp_img').src = "http://(your
Spider IP address)/screenshot.jpg?rnum=" + c;
    c = c + 1
    t = setTimeout("updateSpiderSnapshot()", 60000) // 60 sec
}
updateSpiderSnapshot();
</script>
]]>
</Content>
</Module>

```

4. Upload the edited xml file (**spider1.xml**) to a web server that is accessible over the Internet.
5. Enter the URL **<http://www.google.com/ig>**.
6. Log in to your iGoogle account.
7. Click **Add Stuff**.
8. Click **Add feed or gadget**.
9. Enter the URL **[http://\(your internet web server IP address\)/spider1.xml](http://(your internet web server IP address)/spider1.xml)** and click **Add**.
10. In response to a Google pop-up a warning, click **OK**.
11. Click **Back to homepage**. You should see an iGoogle gadget similar to the following:



# 10: Command Line Interface (CLI)

## Introduction to Commands

### Command Syntax

Commands have the following format:

`<action> <category> <parameter(s)>`

where

`<action>` is set, show, connect, diag, admin, or logout.

`<category>` is a group of related parameters you want to configure or view. Examples are devicegroup, account, and network.

`<parameter(s)>` is one or more name-value pairs in one of the following formats:

<code>&lt;parameter name&gt; &lt;aa bb&gt;</code>	Specify one of the values (aa or bb) separated by a vertical line (   ). The values are all lowercase and must be entered exactly as shown. Bold indicates a default value.
<code>&lt;parameter name&gt; &lt;Value&gt;</code>	Specify an appropriate value, for example, a device group name.  This User Guide shows parameter values in mixed case to indicate they are case sensitive. For example, if you saved a device group name in mixed case, you must enter it in mixed case; if you saved it in lowercase, you must enter it in lowercase.
Square brackets [ ]	Indicate optional parameters.

Figure 10-1. Actions and Category Options

Action	Category
set	sshkey history network
show	sshkey history network
connect	serial
admin	version config
logout	Terminates CLI session.

## Command Help

For general command help, type: **help**

For more information about a specific command, type **help** followed by the command, for example:

```
help set network
```

OR

type **?** after the command:

```
set network ?
```

## Tips

- ◆ Type enough characters to identify the action, category, or parameter name uniquely. For parameter values, type the entire value. For example,
 

```
set network port 1 state static ipaddr 122.3.10.1 mask 255.255.0.0
```

 can be shortened to:
 

```
se net po 1 st static ip 122.3.10.1 ma 255.255.0.0
```
- ◆ Use the **Tab** key to automatically complete action, category, or parameter names. Type a partial name and press **Tab** to complete the name if only one is possible, or to display the possible names if more than one is possible.
- ◆ Should you make a mistake while typing, backspace by pressing the **Backspace** key or the **Delete** key, depending on how you accessed the interface. Both keys work if you use VT100 emulation in your terminal access program when connecting to the console port. Use the **left** and **right arrow** keys to move within a command.
- ◆ Use the **up** and **down arrows** to scroll through previously entered commands. If desired, select one and edit it. You can scroll through up to 100 previous commands entered in the session.
- ◆ When the number of lines displayed by a command exceeds the size of the window (the default is 20), the "Type more to see the next page" message displays. To display the next page, type **more** and press **Enter**. You can override the number of lines (or disable the feature altogether) with the `set cli` command.
- ◆ To clear an IP address, type `0.0.0.0`.

## Configuration Commands

### **admin config**

#### **Syntax**

```
admin config factorydefaults
```

#### **Description**

Restores the SLS configuration and device database settings to factory defaults.

**Note:** *The unit will reboot after this command. All current settings will be lost.*

## Connect Commands

### **connect serial**

#### **Syntax**

```
connect serial
```

#### **Description**

Connects the Spider to a device's serial port.

**Note:** *To connect to a serial port, put the serial port in passthrough mode on the web interface.*

### **ESC exit**

#### **Syntax**

```
ESC exit
```

#### **Description**

Exits a serial port connection.

## SSH Key Commands

### **set sshkey delete**

#### **Syntax**

```
set sshkey delete keyuser <SSH Key User> keyhost <SSH Key Host>
```

#### **Description**

Deletes an imported SSH key.



**Example**

```
set sshkey delete keyuser sysadmin keyhost slm-pipe
```

Deletes imported SSH public key on host *slm-pipe* for the user *sysadmin*.

**set sshkey import****Syntax**

```
set sshkey import <copypaste>
```

Imports public SSH key (OpenSSH format)

**Note:** RSA keys must be 1024 bits

```
set sshkey import <copypaste> format <openssl> keyuser <SSH Key User>
keyhost <SSH Key Host>
```

Imports public SSH key (OpenSSL format)

**Description**

Imports an SSH key.

**Example**

```
set sshkey import copypaste format openssl keyuser sysadmin keyhost
slm-pipe
```

Imports public key in OpenSSL format on host *slm-pipe* for the user *sysadmin*.

**show sshkey import****Syntax**

```
show sshkey import <one or more parameters>
```

**Parameters**

[keyuser <SSH Key User>]

[keyhost <SSH Key IP Address or Name>]

[viewkey <enable|disable>]

**Description**

Displays imported SSH keys.

**Examples**

```
show sshkey viewkey enable
```

Displays all imported SSH public keys with content of keys.

```
show sshkey keyuser sysadmin keyhost slm-pipe
```

Displays imported SSH public key on host *slm-pipe* for the user *sysadmin*.

## History Commands

### **set history clear**

#### **Syntax**

```
set history clear
```

#### **Description**

Clears the CLI command history.

### **show history**

#### **Syntax**

```
show history
```

#### **Description**

Displays the 100 most recent CLI commands.

### **set history clear**

#### **Syntax**

```
set history clear
```

#### **Description**

Clears the CLI command history.

## Network Commands

### **set network gateway**

#### **Syntax**

```
set network gateway <parameters>
```

#### **Parameters**

```
[default <IP Address>]
```

#### **Description**

Configures the network gateway.

**set network setting****Syntax**

```
set network setting <parameters>
```

**Parameters**

```
state <dhcp|bootp|static>
```

```
[ipaddr <IP Address> mask <Mask>]
```

**Description**

Configures network settings.

**show network all****Syntax**

```
show network all
```

**Description**

Displays all network settings.

## Version Command

**admin version****Syntax**

```
admin version
```

**Description**

Displays Spider firmware version information.

## A: Troubleshooting

1. No connection can be established to the Spider

Check cabling. Are both USB cables or all of the USB and PS/2 cables plugged in? Are both Pwr LEDs lit? Is the Ethernet cable plugged in, and the Link light lit? Is there Activity?

Have a look on your network. Verify your network configuration (IP address, router). Send a ping request to the Spider to find out whether the Spider is reachable via the network. Establish a direct connection between the Spider and the client. If you use a firewall then check the appropriate port for accepting connections. The TCP ports 80 (for HTTP) and 443 (for both HTTPS and RFB) have to be open (the server providing the firewall has to accept incoming TCP connections on these ports). You may restrict these connections to the IP addresses used by the Spider and your client.

2. Login on the Spider fails.

Verify both your user login and your password. By default, the user **sysadmin** has the password **PASS**. Ensure the web browser is configured to accept cookies.

3. The Remote Console window of the Spider does not open.

A firewall may prevent access to the Remote Console (TCP port 443). If there is a proxy server between the Spider and your host, then you may not be able to transfer the video data using RFB. Check the settings of the Spider and choose a different server port used for RFB transfer. A Java Runtime Environment may not be installed, or may be disabled.

4. The video quality is bad or the picture is grainy.

Enter the Remote Console and click the **Auto Adjust** button to adjust the Spider's video input parameters to the correct values.

5. Special key combinations (e.g., **ALT+F2**, **ALT+F3**) are intercepted by the client system and not transmitted to the remote computer.

You have to define a Button Key. This can be done in the Remote Console settings. Alternatively, use the soft keyboard feature.

6. The Spider web pages are not displayed correctly.

Check your browser's cache settings. Ensure the cache settings are not set to "do not check for newer pages." Otherwise the web pages may be loaded from your browser cache and not from the Spider.

7. Every time I open a dialog box with some buttons, the mouse pointers are not synchronous anymore.

Disable the setting **Automatically move mouse pointer to the default button of dialog boxes** in the mouse settings of your operating system.

8. The Remote Console does not open with Opera in Linux.

Some versions of Opera do not grant enough permission if the signature of the applet cannot be verified. To solve the problem, add the lines `grantcodeBase "nn.pp.rc.RemoteConsoleApplet" {permission java.lang.RuntimePermission "accessClassInPackage.sun.*";` to the java policy file of opera (e.g., `/usr/share/opera/java/opera.policy`).

9. I forgot my password. How can I reset the Spider to factory defaults?

Use the serial interface with a terminal emulator program set to 115200, 8, None, 1, No flow control. Within 2 seconds of booting the Spider, enter the **Esc** key a few times to get a **➔** prompt. Enter **Defaults**.

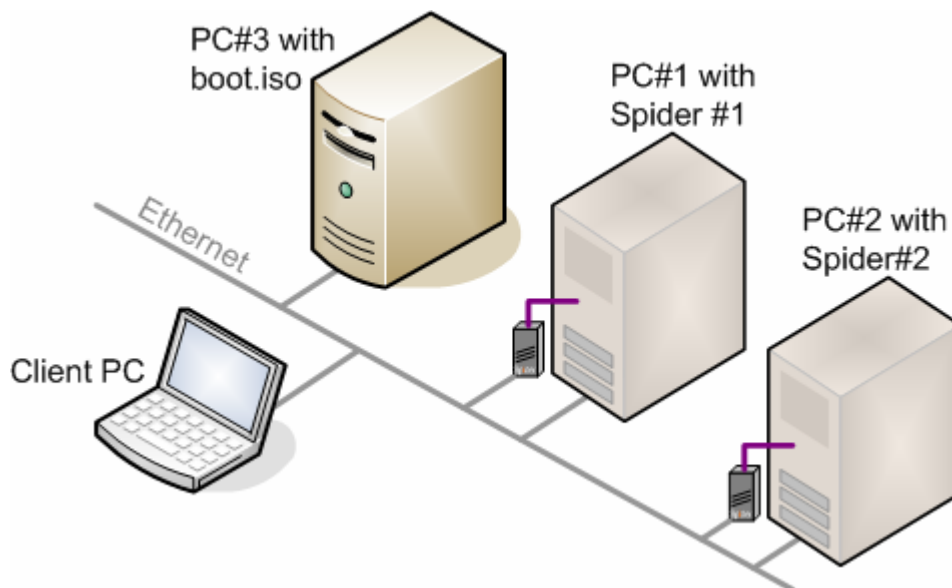
10. Cannot upload the signed SSL certificate in MacOS X.

If an "internal error" occurs while uploading the signed certificate either changes the extension of the file to .txt or adds a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is set to "plain text" and the checkbox "use for outgoing" is set. As an alternative, you may also use a Mozilla based browser (Mozilla, FireFox).

## B: Virtual Media Example

### Goal

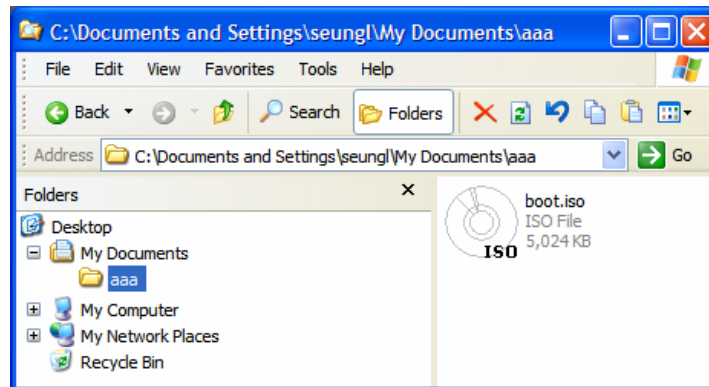
In this example, the goal is to put a rescue CD (a CD used to boot a PC when the hard-disk corruption prevents OS boot) on PC#3 so that the rescue CD can be used by any Spiders on the network.



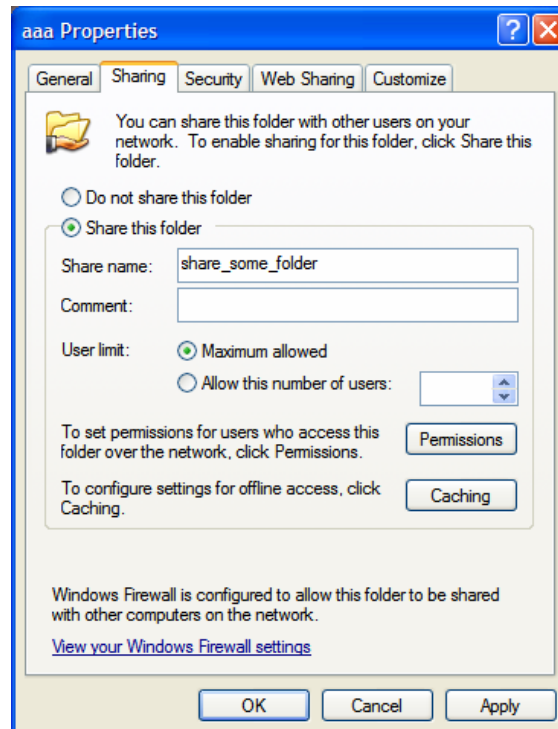
In this example, PC#2 cannot boot from its hard disk, so the user wants to use the rescue CD to boot the PC. We assume PC#2 can boot from external USB device.

## Step 1 – Prepare the VM Server

1. Use any CD-copy application to create an ISO image of the rescue CD, and call this ISO image file `boot.iso`.
2. On PC#3 (Windows XP in this example), put the ISO file in a Windows folder – file `boot.iso` in folder `aaa` as shown in the diagram below.



3. Right-click the folder `aaa` and select the “sharing” menu. The default name is the folder name but changed to `share_some_folder` as shown in the diagram below.



Now, the file `boot.iso` can be used from a Spider. The file can be left there permanently, and when a PC/server crashes and cannot boot, the combination of this file and the Spider will be used to boot the PC/server.

## Step 2 – Enable Virtual Media

In this example, PC#2 does not respond, and rebooting does not cure the problem. PC#2 has Spider#2 attached.

1. On any PC (call this the client PC), bring up a browser, browse to Spider#2, and log in.
2. Go to the Virtual Media page and complete the fields in the **Image on Windows Share** section of the page as shown in the diagram below.

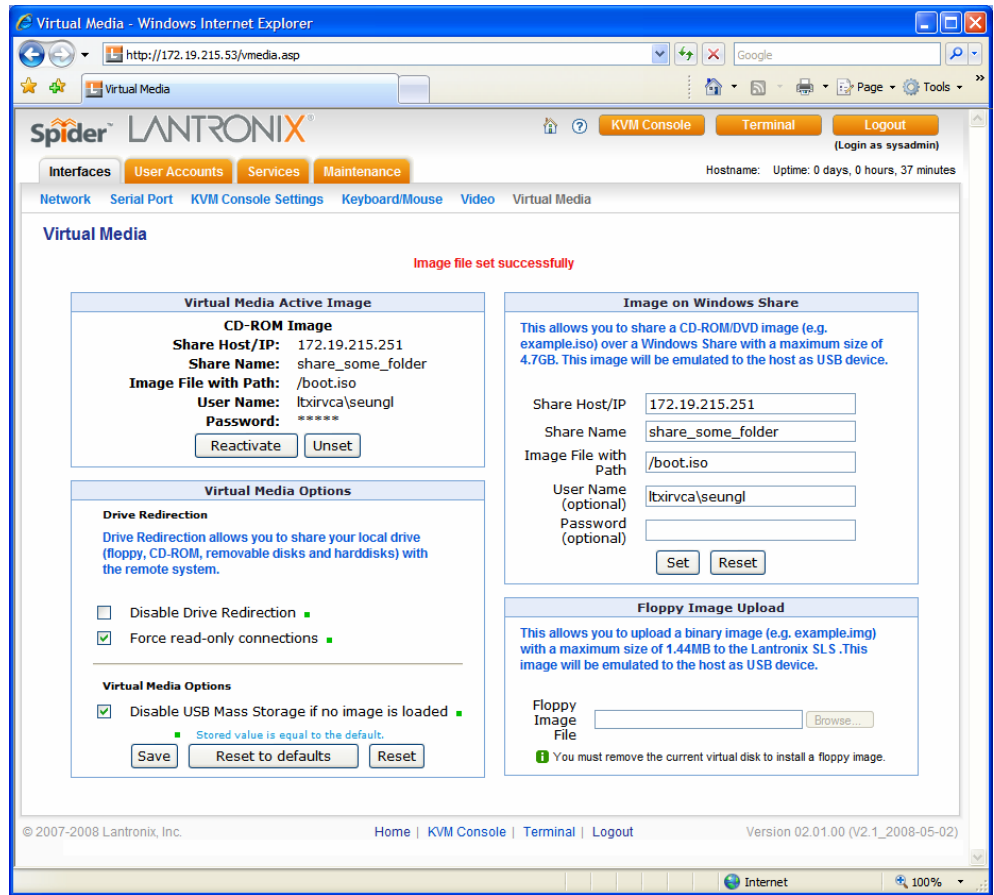
The screenshot shows the Spider Lantronix Virtual Media configuration page. The browser window title is "Virtual Media - Windows Internet Explorer" and the address bar shows "http://172.19.215.53/vmedia.asp". The page has a navigation bar with tabs: Interfaces, User Accounts, Services, Maintenance, Network, Serial Port, KVM Console Settings, Keyboard/Mouse, Video, and Virtual Media. The "Virtual Media" tab is selected. The page content is divided into several sections:

- Virtual Media Active Image:** A status box indicating "No disk emulation set."
- Virtual Media Options:**
  - Drive Redirection:** A section explaining that drive redirection allows sharing local drives (floppy, CD-ROM, removable disks, and harddisks) with the remote system. It includes two checkboxes: "Disable Drive Redirection" (unchecked) and "Force read-only connections" (checked).
  - Virtual Media Options:** A section with a checkbox "Disable USB Mass Storage if no image is loaded" (checked). Below it, a note states "Stored value is equal to the default." There are "Save", "Reset to defaults", and "Reset" buttons.
- Image on Windows Share:** A section explaining that this allows sharing a CD-ROM/DVD image (e.g., example.iso) over a Windows Share with a maximum size of 4.7GB. It includes fields for:
  - Share Host/IP: 172.19.215.251
  - Share Name: share\_some\_folder
  - Image File with Path: /boot.iso
  - User Name (optional): ltxirvca\seungr
  - Password (optional): [masked]
 There are "Set" and "Reset" buttons.
- Floppy Image Upload:** A section explaining that this allows uploading a binary image (e.g., example.img) with a maximum size of 1.44MB to the Lantronix SLS. It includes a "Floppy Image File" input field with a "Browse..." button and an "Upload" button.

The footer of the page includes copyright information "© 2007-2008 Lantronix, Inc.", navigation links "Home | KVM Console | Terminal | Logout", and version information "Version 02.01.00 (v2.1\_2008-05-02)".

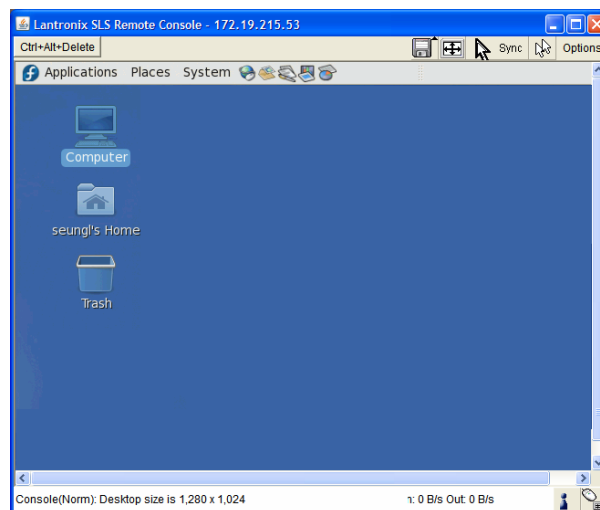


- Click **Set**, and see that the **Virtual Media Active Image** section now contains data as shown in the diagram below.

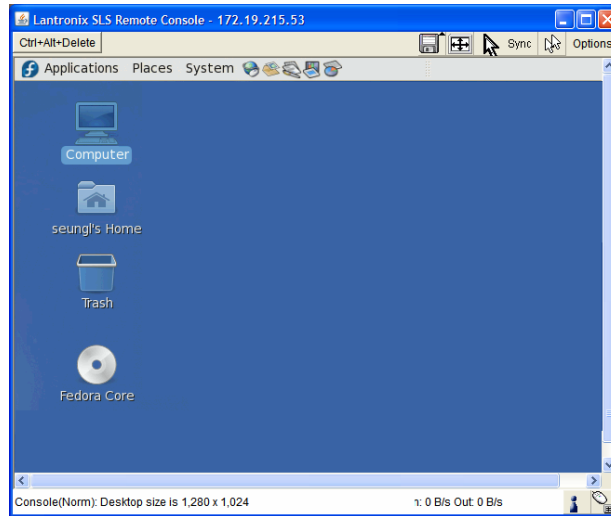


## Step 3 – Use the Virtual Media

PC#2 shown in the diagram below is a Linux PC.



Once step 2 is done, PC#2 will detect a new USB CD drive connected to its USB as shown in the diagram below. The CD is shown below as **Fedora Core** because that is the volume name of the rescue CD (`boot.iso` is the ISO image of this CD).



You should be able to boot from the external USB device (`boot.iso`) on PC#2. Make sure that you set BIOS to boot from the USB device.

## C: Supported Video Formats

The following table displays supported video formats for the Spider:

Resolution (x,y)	Refresh Rates (Hz)
640x340	70, 85
640x400	56, 85
640x480	60, 67, 72, 75, 85
720x400	70, 85
800x600	56, 60, 70, 72, 75, 85
832x624	75
1024x768	60, 70, 72, 75, 85
1152x864	75
1152x870	75
1152x900	66, 76
1280x960	60
1280x1024	60

## D: Mounting Bracket Kit for the Spider (083-015-R)

A versatile mounting bracket and screws are supplied to assist in easily installing and mounting a single Spider into a server rack in various orientations (e.g., horizontal or vertical).

The kit includes:

- ◆ One (1) 4.0" x 1-3/4" x 1/4" bracket
- ◆ Two (2) 1/2" long, 10-32 stainless steel Phillips-head screws



Once the mounting bracket is installed in the rack, the Spider can be easily and securely attached to the bracket's elevated mounting posts, and easily removed if necessary.

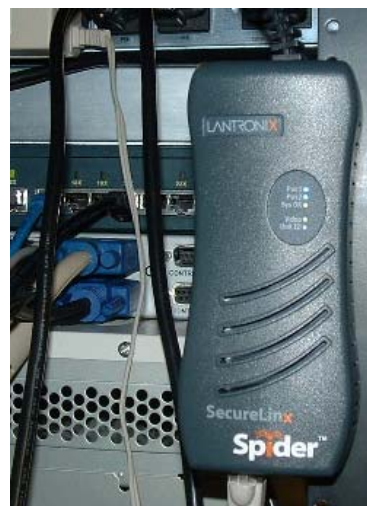
There are only 3 easy steps to install the mounting bracket and Spider into a server rack:



1. Mount the bracket with a Phillips-head screwdriver



2. Attach the Spider to the bracket's mounting posts



3. Connect cables and the Spider is ready for use!

Lantronix Part Number	Description
083-015-R	Mounting Bracket Kit for Spider

The bracket kit is included in the box with Spiders that ship with v2.0 firmware and later. For earlier shipments, the mounting kit is sold separately. For additional information contact Lantronix Sales at 800-422-7055, or for technical questions contact Lantronix Technical Support at <http://www.lantronix.com/support>.

## ***E: Technical Support and Warranty***

### **Technical Support**

If you are unable to resolve an issue using the information in this documentation:

#### **Technical Support US**

Check our online knowledge base or send a question to Technical Support at <http://www.lantronix.com/support>.

Phone: (949) 422-7044  
(949) 453-7198

#### **Technical Support Europe, Middle East, Africa**

Phone: +33 1 39 30 41 72

Email: [mailto:eu\\_techsupp@lantronix.com](mailto:eu_techsupp@lantronix.com) or [mailto:eu\\_support@lantronix.com](mailto:eu_support@lantronix.com)

Firmware downloads, FAQs, and the most up-to-date documentation are available at <http://www.lantronix.com/support>

When you report a problem, please provide the following information:

- ◆ Your name, and your company name, address, and phone number
- ◆ Lantronix model number
- ◆ Lantronix serial number
- ◆ Firmware version
- ◆ Description of the problem
- ◆ Target computer interface (PS/2 or USB) and video format
- ◆ Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

### **Warranty**

For details on the Lantronix warranty replacement policy, go to our web site at [www.lantronix.com/support/warranty](http://www.lantronix.com/support/warranty).

## ***F: Compliance***

(according to ISO/IEC Guide 22 and EN 45014)

### **Manufacturer's Name & Address:**

Lantronix Inc., 15353 Barranca Parkway, Irvine, CA 92618 USA

*Declares that the following product:*

### **Product Name(s): SecureLinx Spider**

*Conform to the following standards or other normative documents:*

- ◆ UL/CUL (CSA-22.2 No. 60950-1-03 / UL-60950-1)
- ◆ CE - IEC 60950-1
- ◆ C-Tick
- ◆ FCC Part 15, Equipment Class A
- ◆ VCCI V-3/2006.04 Class A
- ◆ AS/NZS CISPR 22: 2006 Class A
- ◆ EN55022:1998 +A1:2000 +A2:2003 Class A
- ◆ EN61000-3-2: 2000 +A2: 2005 Class A
- ◆ EN61000-3-3: 1995 +A1: 2001
- ◆ EN55024: 1998 +A1:2001 +A2:2003
- ◆ Pb-free components

## RoHS Notice:

All Lantronix products in the following families are China RoHS-compliant and free of the following hazardous substances and elements:

- Lead (Pb)
- Mercury (Hg)
- Polybrominated biphenyls (PBB)
- Cadmium (Cd)
- Hexavalent Chromium (Cr (VI))
- Polybrominated diphenyl ethers (PBDE)

Product Family Name	Toxic or hazardous Substances and Elements					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent Chromium (Cr (VI))	Polybrominated biphenyls (PBB)	Polybrominated diphenyl ethers (PBDE)
UDS1100 and 2100	0	0	0	0	0	0
EDS	0	0	0	0	0	0
MSS100	0	0	0	0	0	0
IntelliBox	0	0	0	0	0	0
XPress DR & XPress-DR+	0	0	0	0	0	0
SecureBox 1101	0	0	0	0	0	0
WiBox	0	0	0	0	0	0
UBox	0	0	0	0	0	0
MatchPort	0	0	0	0	0	0
SLC	0	0	0	0	0	0
XPort	0	0	0	0	0	0
WiPort	0	0	0	0	0	0
SLB	0	0	0	0	0	0
SLP	0	0	0	0	0	0
SCS	0	0	0	0	0	0
SLS	0	0	0	0	0	0

O: toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

X: toxic or hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in SJ/T11363-2006.